Share and Share Alike: Intelligence Agencies and Information Sharing

Nathan Alexander Sales*

Table of Contents

Introduction

Information sharing is the one counterterrorism initiative virtually everyone supports. Yet no one seems to have any idea how to make it happen.

Like the American public as a whole, the academy remains divided on the wisdom and legality of many measures undertaken in the

* Assistant Professor of Law, George Mason University School of Law. I'm indebted, for their helpful comments, to Stewart Baker, Bill Banks, Nate Cash, Bobby Chesney, Peyton Cooke, Bruce Johnsen, Bruce Kobayashi, Greg McNeal, Adam Mossoff, Sam Vermont, Matt Waxman, and Todd Zywicki, as well as participants in the 2009 National Security Law Workshop at the University of Texas School of Law. Special thanks to the Center for Infrastructure Protection for generous financial support. I worked on a number of information-sharing initiatives while serving at the Departments of Justice and Homeland Security, but the opinions expressed in this article are solely mine.

name of national security since the terrorist attacks of September 11, 2001. Sharp disputes persist over lengthy detentions of suspected terrorists outside the criminal-justice system, coercive interrogations of captured al Qaeda leaders and other detainees, and eavesdropping on Americans' international communications without court orders. Yet the need for more effective information sharing remains a rare area of agreement, both within academia[1] and without.[2] Of course there are exceptions.[3] There always are. Still, the consensus in favor of more information sharing has proven surprisingly broad and durable.

Egged on by the commentariat, Congress and the executive branch have enacted a series of measures intended both to eliminate legal restrictions on information sharing and to promote data exchange among national security players. For example, in 2001, Con-

---

1 *See, e.g.*, RICHARD A. POSNER, PREVENTING SURPRISE ATTACKS: INTELLIGENCE REFORM IN THE WAKE OF 9/11 at 26, 28 (2005) [hereinafter POSNER, SURPRISE ATTACKS]; Noah Feldman, *Choices of Law, Choices of War*, 25 HARV. J.L. & PUB. POL'Y 457, 482 (2002); Michael V. Hayden, *Balancing Security and Liberty: The Challenge of Sharing Foreign Signals Intelligence*, 19 NOTRE DAME J.L. ETHICS & PUB. POL'Y 247, 257–60 (2005); David S. Kris, *The Rise and Fall of the FISA Wall*, 17 STAN. L. & POL'Y REV. 487, 518, 521–22 (2006); Craig S. Lerner, *The USA PATRIOT Act: Promoting the Cooperation of Foreign Intelligence Gathering and Law Enforcement*, 11 GEO. MASON L. REV. 493, 524–26 (2003); Richard Henry Seamon & William Dylan Gardner, *The PATRIOT Act and the Wall Between Foreign Intelligence and Law Enforcement*, 28 HARV. J.L. & PUB. POL'Y 319, 458–63 (2005); Peter P. Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 VILL. L. REV. 951, 951–59 (2006).

2 *See, e.g.*, COMM'N ON THE INTELLIGENCE CAPABILITIES OF THE U.S. REGARDING WEAPONS OF MASS DESTRUCTION, REPORT TO THE PRESIDENT OF THE UNITED STATES 429–50 (2005) [hereinafter WMD REPORT]; MARKLE FOUND., CREATING A TRUSTED INFORMATION NETWORK FOR HOMELAND SECURITY: SECOND REPORT OF THE MARKLE FOUNDATION TASK FORCE (2003); MARKLE FOUND., MOBILIZING INFORMATION TO PREVENT TERRORISM: ACCELERATING DEVELOPMENT A TRUSTED INFORMATION SHARING ENVIRONMENT, THIRD REPORT OF THE MARKLE FOUNDATION TASK FORCE (2006) [hereinafter THIRD MARKLE REPORT]; MARKLE FOUND., NATION AT RISK: POLICY MAKERS NEED BETTER INFORMATION TO PROTECT THE COUNTRY (2009) [hereinafter FOURTH MARKLE REPORT]; MARKLE FOUND., PROTECTING AMERICA'S FREEDOM IN THE INFORMATION AGE: A REPORT OF THE MARKLE FOUNDATION TASK FORCE (2002) [hereinafter FIRST MARKLE REPORT]; NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 416–19 (2004) [hereinafter 9/11 COMMISSION REPORT].

3 *See, e.g.*, POSNER, SURPRISE ATTACKS, *supra* note 1, at 40 (arguing that the 9/11 Commission's report "identifies no *current* impediments to the flow of information within and among intelligence agencies concerning Islamist terrorism" and suggesting that "sharing is not a problem after all"); William C. Banks, *And the Wall Came Tumbling Down: Secret Surveillance After the Terror*, 57 U. MIAMI L. REV. 1147, 1150 (2003) (accepting the need for more sharing but describing efforts to promote coordination between intelligence and law-enforcement officials as "overreaching"); Jennifer M. Collins, *And the Walls Came Tumbling Down: Sharing Grand Jury Information with the Intelligence Community Under the USA PATRIOT Act*, 39 AM. CRIM. L. REV. 1261, 1270–86 (2002) (arguing that prosecutors should be allowed to share grand-jury information with intelligence analysts, but only with prior judicial approval).

gress allowed federal prosecutors to share information uncovered in grand-jury investigations and through wiretaps with their counterparts in the intelligence community.[4] A year later, Congress directed federal agencies to exchange "homeland security information" with one another.[5] And in 2004, the government established an "information sharing environment" to encourage the free flow of national security data.[6]

Despite a decade of effort, however, there is a widespread sense that information sharing is "going nowhere."[7] Why?

Because policymakers have failed to account for the iron law of agency self-interest.[8] Reformers have repealed a number of legal impediments to data exchange, and they have exhorted intelligence agencies to do a better job of sharing. But they have done little to eliminate the natural bureaucratic incentives that dissuade agencies from cooperating with one another. Nor have policymakers fostered new incentives to encourage agencies to exchange data. No matter how many bills are passed or executive orders signed, intelligence agencies won't connect the dots unless it's in their interest to do so. It's not enough simply to tear down the wall. Agencies must be given reasons to climb over the rubble.[9]

---

4 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 203, 115 Stat. 272, 278–81.

5 Homeland Security Act of 2002, Pub. L. No. 107-296, § 892, 116 Stat. 2135, 2253–55.

6 Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1016(b), 118 Stat. 3638, 3665–66.

7 RICHARD A. POSNER, UNCERTAIN SHIELD: THE U.S. INTELLIGENCE SYSTEM IN THE THROES OF REFORM 79 (2006) [hereinafter POSNER, UNCERTAIN SHIELD]; *see also, e.g.*, WMD REPORT, *supra* note 2, at 320 ("While minor advances have been made in some areas, the ultimate objective of developing a Community-wide space for sharing intelligence information has proven elusive."); FOURTH MARKLE REPORT, *supra* note 2, at 4 (warning that "old habits die hard" and that "stovepiping of information within agencies persist[s]"); Mark Mazzetti, *Report Faults Spy Chief for Inaction on Turf Wars*, N.Y. TIMES, Apr. 2, 2009, at A15 (reporting finding of the Office of the Director of National Intelligence Inspector General that "'the culture of protecting 'turf' remains a problem, and there are few, if any, consequences for failure to collaborate'").

8 *Cf.* Daryl J. Levinson, *Empire-Building Government in Constitutional Law*, 118 HARV. L. REV. 915, 925 (2005) (emphasizing that "predictions about the behavior of government institutions ought to rest on plausible accounts of the interests of individual officials who direct these institutions").

9 *Cf.* Banks, *supra* note 3, at 1172 (arguing that "problems of coordination and cooperation" among intelligence agencies "are more institutional and cultural than legal," and proposing that "[r]eforms of the institutional culture would better ensure counterterrorism objectives than stretching the legal safeguards"); Lerner, *supra* note 1, at 505 (describing statutory reforms as "parchment attacks on embedded cultural norms").

Hence this article, the first comprehensive analysis of why intelligence agencies fail to share information and what may be done about it.

Part I recounts a number of recent information-sharing failures. Some are notorious, others obscure. Some are operational missteps—such as CIA's refusal in 2001 to alert other agencies that an al Qaeda member (and eventual 9/11 hijacker) had entered the United States. Others are failures of policy—for example, the Justice Department's decision to erect a "wall" between intelligence officials at the FBI and their law-enforcement counterparts. Part I then describes the major post-9/11 legislative and executive initiatives to correct these problems.

Part II consults public-choice principles and insights from other legal disciplines to explain why intelligence agencies tend to hoard information. It begins by asking: What do agencies maximize? The answer, I suggest, is twofold. Intelligence agencies seek to maximize their influence over senior policymakers in the executive branch, as well as their autonomy—i.e., the ability to pursue agency priorities without outside interference. Information sharing can undermine both goods. Data exchange can lead to free riding and, with it, a loss of relative influence; if the FBI shares information with CIA, policymakers might give credit to CIA for any resulting intelligence breakthroughs. Agencies also fear that information sharing will enable their rivals to muscle in on their turf, such as by seizing control of an ongoing operation.

Part II then proposes a series of analytical frameworks, or lenses, through which agencies' tendency to hoard might be understood. First, data exchange sometimes resembles an intellectual-property ("IP") problem. Agencies treat their intelligence information like private firms treat trade secrets. As in the private sector, sensitive information is valuable to an agency only to the extent it is able to shield that data from competitors. If the FBI free rides on CIA data, it might enhance its own influence and cause CIA's to wane. Antitrust law supplies a second lens. An agency's reluctance to share information with rivals can be thought of as the bureaucratic equivalent of a refusal to deal. Intelligence agencies also engage in familiar forms of rent seeking, such as lobbying the President to grant them monopoly rights in various intelligence submarkets. And they form cartels to enforce market-division arrangements, insulating themselves against competition in their respective market niches. Organizational theory is a third lens through which to view the hoarding problem. Intelli-

gence officials are conditioned by an institutional culture of risk aversion, which stems from the asymmetries between their career rewards and penalties. They almost always stand to lose more from bold and independent action than they stand to gain, and so they have strong incentives to keep their information to themselves. Analysts are well aware that, as an FBI supervisor warned in the 1990s, information sharing can be a "'career stopper.'"[10]

Part III considers how to adjust the incentive structure to encourage agencies to share—and to do so in a way that doesn't weaken their existing incentives to collect information in the first place. In particular, it examines whether intellectual-property, antitrust, and organizational-theory solutions could be adapted for the information-sharing context. Policymakers might replace the trade-secrets regime that currently governs intelligence products with a system based on patent and copyright principles. That could be accomplished by requiring agencies to somehow publish their intelligence data as a precondition of receiving IP-type protections, or by subjecting them to a copyright-style compulsory licensing scheme. To mitigate free-riding concerns, originating agencies could be offered various kinds of compensation when rivals use their products. Policymakers also might look to antitrust law's suite of enforcement tools. They could establish a central regulator with the power to impose sanctions (monetary and otherwise) on agencies that refuse to share. They could create a mechanism for individual intelligence agencies to litigate challenges to their rivals' efforts to hoard. And they could harness market forces to promote information sharing, such as by relaxing the intelligence market's severe entry barriers. Finally, policymakers could mitigate intelligence agencies' cultural risk aversion by creating new, pro-sharing incentives. They could increase the benefits an individual analyst could expect to gain from sharing (such as by offering cash bounties) while decreasing the expected costs of doing so (such as by eliminating legal ambiguities about which kinds of information may be shared and which may not).

A few qualifications are needed. This Article does not engage the underlying policy question of whether information sharing is in fact desirable. Instead, it takes the general consensus in favor of expanded data exchange for granted, and then considers the reasons agencies tend to hoard and what solutions might encourage them to share. It should be emphasized that intelligence agencies sometimes

---

10 *See* Kris, *supra* note 1, at 501; *see also* 9/11 COMMISSION REPORT, *supra* note 2, at 79.

will have compelling reasons not to share a particular piece of information. For instance, sharing might compromise a sensitive source or method—"information about the manner in which the government collects intelligence," such as the identities of spies, electronic-surveillance capabilities, and so on.[11] While I assume that information sharing is generally advisable, it is not invariably so in all circumstances.

In addition, this article focuses primarily on challenges associated with "horizontal" information sharing—the exchange of data among peers (e.g., between one federal agency and another, or between the United States and a foreign government). It largely ignores the different problems posed by "vertical" information sharing—the flow of data within a hierarchical system (e.g., between the federal government and the states, or between intelligence analysts and their supervisors). This Article likewise is limited to the sharing of "strategic" or "analytical" intelligence—data about hostile powers' capabilities and intentions. It does not address the sharing of "tactical" or "operational" intelligence—data about ongoing national security operations, such as plans to take an al Qaeda suspect into custody or conditions that prevail on a battlefield.[12] Finally, writing about highly secretive intelligence matters is fraught with difficulty. Some information about agencies' sharing practices is a matter of public record, but a great deal presumably remains classified. Given the asymmetry between reality and reality as publicly reported, this Article's conclusions are necessarily tentative.

I. A Page of History: Failures and Fixes

If information sharing is such a great idea, why isn't there more of it? This section discusses some representative failures by intelligence agencies to share information in recent years. Some of the missteps are the result of programmatic policy choices; others are ad hoc and situational. This is not a normative exercise. The point is not to

---

11 Nathan Alexander Sales, *Secrecy and National Security Investigations*, 58 ALA. L. REV. 811, 818 (2007); *see also* CIA v. Sims, 471 U.S. 159, 167 (1985) (describing sources and methods as "the heart of all intelligence operations").

12 Intelligence agencies may have even stronger incentives to hoard tactical/operational data than strategic/analytical data, and they may be more justified in doing so. This is due to the greater costs agencies incur from the compromise of tactical information. If an agency shares strategic intelligence that leaks, it faces the loss of sensitive sources and methods. But if tactical intelligence leaks—e.g., the FBI's plans to arrest a terrorism suspect, or the Navy's plans for a cruise missile strike on an al Qaeda camp—not only will the agency's sources and methods suffer, the operation itself might be compromised. The suspect may flee, and the camp may relocate. *See* Sales, *supra* note 11, at 821.

blame any particular agency for hoarding, still less for any resulting intelligence failures. Rather, the objective is to lay a descriptive foundation so we can begin to understand how hoarding results from intelligence agencies' rational pursuit of their respective interests. Part I then moves on to describe responses to these shortcomings by policymakers on Capitol Hill and in the White House.

A. Information-Sharing Missteps

1. Something There Is That Doesn't Love a Wall[13]

Perhaps the most notorious legal restriction on information sharing is the infamous "wall" between intelligence officials and criminal investigators.[14] The wall—codified in a series of internal Department of Justice ("DOJ") guidelines that in turn were based on an analysis of the federal statutes governing electronic surveillance—effectively barred the FBI's intelligence officials from exchanging data or otherwise coordinating with their law-enforcement counterparts at DOJ.[15] The USA PATRIOT Act set out to destroy the wall, and, with an assist from a specialized federal appellate court, largely succeeded in doing so.[16] Though the wall has come down,[17] it remains a useful vehicle for understanding why administrative agencies are reluctant to share with one another.[18]

The origins of the wall lie in the Foreign Intelligence Surveillance Act of 1978[19] ("FISA"), which regulates the government's ability to conduct electronic surveillance in certain types of national security investigations.[20] As originally enacted, FISA required the government to certify to the Foreign Intelligence Surveillance Court that "the pur-

---

13 Robert Frost, *Mending Wall*, *in* THE POETRY OF ROBERT FROST 33, 33 (Edward Connery Lathem ed., Henry Holt 1979).

14 Other walls exist. *See infra* notes 253–57 and accompanying text.

15 Originally, the wall was internal to the Justice Department; its principal function was to separate the FBI's intelligence officials from criminal investigators at Main Justice. *See* Kris, *supra* note 1, at 499–508. Later, the term came to mean restrictions on intelligence and law enforcement more generally. *See* Seamon & Gardner, *supra* note 1, at 323 n.13.

16 *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("USA PATRIOT Act") Act of 2001, Pub. L. No. 107-56, § 218, 115 Stat. 272, 291 (codified at 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B) (2006)); *In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002).

17 *See infra* notes 111–14 and accompanying text.

18 For histories of the wall, see 9/11 COMMISSION REPORT, *supra* note 2, at 78–80; Banks, *supra* note 3, at 1153–88; Kris, *supra* note 1, at 499–518; Lerner, *supra* note 1, at 495–512; Seamon & Gardner, *supra* note 1, at 358–80.

19 Foreign Intelligence Surveillance Act (FISA) of 1978, Pub. L. No. 95-511, 92 Stat. 1783.

20 FISA generally requires the government to establish, among other things, probable cause to believe that the target of the proposed electronic surveillance is "a foreign power or an

pose" of proposed surveillance was "to obtain foreign intelligence."[21] If the purpose was anything else—for example, accumulating evidence for use in a criminal prosecution of health-care fraud—FISA's relatively relaxed authorities were off the table. The government would have to make do with the comparatively rigorous standards spelled out in the federal wiretap statute, known as Title III.[22] The concern was with ensuring that the government didn't use FISA to circumvent Title III (and the Fourth Amendment values it reinforced).[23] Over the years, Congress,[24] the executive branch,[25] and federal courts[26] alike applied interpretive glosses that softened FISA's purpose test. Under these interpretations, FISA surveillance was permissible whenever "the primary purpose" of the surveillance was foreign intelligence gathering.[27] Foreign intelligence didn't need to be *the* reason—by implication, the *only* reason. Instead, the FISA court could approve a wiretap even if law-enforcement purposes were mixed in with the foreign-intelligence considerations.[28] As long as foreign intelligence gathering was the predominant reason for the surveillance, the presence of ancillary law-enforcement purposes would not disqualify the government from using FISA. Now the feds could take their whiskey with a splash of soda.

---

agent of a foreign power" (e.g., a Soviet spy, or a member of an international terrorist group like al Qaeda). 50 U.S.C. § 1805(a)(3) (2006); *see generally* Sales, *supra* note 11, at 839–49.

21 50 U.S.C. § 1804(a)(7)(B) (2000) (amended 2001).

22 *See* 18 U.S.C. §§ 2510–2522 (2006).

23 *See* Lerner, *supra* note 1, at 497–98.

24 *See, e.g.*, H.R. REP. NO. 95-1283, pt. 1, at 36 (1978) ("[FISA surveillances] are not primarily for the purpose of gathering evidence of a crime. They are to obtain foreign intelligence information.").

25 *See, e.g.*, Memorandum from Jamie S. Gorelick, Deputy Attorney Gen., to Mary Jo White, United States Attorney, S. Dist. N.Y., et al., Instructions on Separation of Certain Foreign Counterintelligence and Criminal Investigations 2, *available at* http://www.cnss.org/1995%20Gorelick%20Memo.pdf [hereinafter Gorelick Memo] ("[T]he primary purpose of the counterintelligence investigation will be to collect foreign counterintelligence information.").

26 *See, e.g.*, United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991) ("Although evidence obtained under FISA subsequently may be used in criminal prosecutions, the investigation of criminal activity cannot be the primary purpose of the surveillance."), *cert. denied*, 506 U.S. 816 (1992); United States v. Megahey, 553 F. Supp. 1180, 1190 (E.D.N.Y. 1982) (holding that FISA surveillance is "appropriate only if foreign intelligence surveillance is the Government's primary purpose"), *aff'd sub nom.* United States v. Duggan, 743 F.2d 59 (2d Cir. 1984); *cf.* United States v. Truong Dinh Hung, 629 F.2d 908, 915 (4th Cir. 1980) (holding, with respect to a pre-FISA wiretap, that the government need not obtain a warrant if "the object of the search or the surveillance is a foreign power, its agents or collaborators" and "the surveillance is conducted 'primarily' for foreign intelligence reasons").

27 *See* Banks, *supra* note 3, at 1157.

28 *See* Lerner, *supra* note 1, at 498–99.

The question then became: How do you know the purpose of a proposed wiretap? The Justice Department's answer was the more coordination between law-enforcement personnel and intelligence officials—between cops and spies—the less likely it is that foreign intelligence is the primary purpose of the surveillance.[29] In other words, information sharing was a proxy for purpose. Justice Department cops and spies therefore were segregated to reduce the risk that the FISA court would deem the primary purpose of surveillance to be something other than foreign intelligence gathering.[30]

In particular, DOJ issued two sets of guidelines in 1995 that were applied in a way that effectively isolated intelligence officials from their law-enforcement counterparts. The first applied to the criminal and intelligence investigations of the 1993 attack on the World Trade Center. The purpose of the guidelines, which DOJ acknowledged "go beyond what is legally required," was to "clearly separate the counterintelligence investigation from the more limited . . . criminal investigations," and thereby "prevent any risk of creating an unwarranted appearance that FISA is being used to avoid procedural safeguards which would apply in a criminal investigation."[31] Therefore, data uncovered by intelligence officials—"including all foreign counterintelligence relating to future terrorist activities"—"will not be provided either to the criminal agents, the [U.S. Attorney's office], or the Criminal Division" except in special circumstances.[32]

The second set of guidelines applied more broadly to all Justice Department intelligence operations.[33] The guidelines stated categorically that law-enforcement officials "shall not . . . instruct the FBI on the operation, continuation, or expansion of FISA electronic surveillance."[34] They went on to direct intelligence and criminal investigators to avoid "either the fact or the appearance of the Criminal Division's directing or controlling the [foreign intelligence] or [foreign counterintelligence] investigation toward law enforcement objec-

---

29 *See* Kris, *supra* note 1, at 497–99.

30 *Id.* at 499–501.

31 Gorelick Memo, *supra* note 25, at 2.

32 *Id.* at 3.

33 Memorandum from Janet Reno, Attorney General, to Assistant Attorney General et al. (July 19, 1995) § (A)(6), *available at* http://www.fas.org/irp/agency/doj/fisa/1995procs.html [hereinafter Reno Memo]. This second set of guidelines was largely reaffirmed in 2001 by President George W. Bush's Justice Department. *See* Memorandum of Larry D. Thompson to Michael Chertoff, Assistant Attorney General, et al. 1 (Aug. 6, 2001), *available at* http://*www.usdoj.gov/dag/readingroom/dag-memo-08062001.pdf* ("The 1995 Procedures remain in effect today.").

34 Reno Memo, *supra* note 33, § (A)(6).

tives."[35] And, as a prophylactic measure, the guidelines directed that the FISA court be informed "of the existence of, and basis for, any contacts among" the Justice Department's cops and spies.[36] The guidelines came to be understood—or misunderstood[37]—as prohibiting officials "from passing nearly all information between investigations of criminal wrongdoing and investigations designed to gather intelligence about potential terrorist activity."[38]

The wall was not intended to be impregnable. A mechanism existed by which FBI intelligence officials could throw information over the wall to their counterparts in the Justice Department's Criminal Division or in U.S. Attorney's offices. The 1995 guidelines directed that if, in the course of FISA surveillance, "facts or circumstances are developed that reasonably indicate that a significant federal crime has been, is being, or may be committed," the FBI was required to share the information with the Criminal Division.[39] In return, criminal investigators could "give guidance to the FBI aimed at preserving the option of a criminal prosecution," such as "advice on the handling of sensitive human sources."[40] The problem was that this sharing mechanism proved cumbersome. Information could not be passed directly from spy to cop. It had to be routed through the Office of Intelligence Policy and Review, a DOJ component responsible for reviewing and submitting surveillance applications to the FISA court.[41] That made bulk data sharing virtually impossible; information could be exchanged only one piece at a time. Even worse, sharing could only be initiated by intelligence officials; there was no way for law-enforcement personnel to do so.[42] As a result, "intelligence coordination with law enforcement dropped off after issuance of the 1995 guidelines, and the contact that did occur came so late in the process as to be practically useless."[43]

---

35 *Id.*

36 *Id.* § (A)(7).

37 *See, e.g.*, 9/11 COMMISSION REPORT, *supra* note 2, at 78–80.

38 AMY B. ZEGART, SPYING BLIND 139 (2007).

39 Reno Memo, *supra* note 33, § (A)(1); *cf.* Gorelick Memo, *supra* note 25, at 3 (directing the FBI to notify criminal investigators if, during an intelligence investigation, "facts or circumstances are developed that reasonably indicate that a significant federal crime has been, is being, or may be committed").

40 Reno Memo, *supra* note 33, § (A)(6).

41 *See* 9/11 COMMISSION REPORT, *supra* note 2, at 78.

42 *See id.* ("Whether the FBI shared with prosecutors information pertinent to possible criminal investigations was left solely to the judgment of the FBI.").

43 Banks, *supra* note 3, at 1162; *see also* Seamon & Gardner, *supra* note 1, at 371.

2. *The Summer of Threat*

Not all failures to share are the result of deliberate policy choices. Sometimes agencies hoard for more ad hoc reasons. Consider CIA's decision to withhold information from the FBI and State Department about a handful of al Qaeda operatives in the run-up to 9/11.[44] CIA knew that Nawaf al Hazmi and Khaled al Mihdhar were al Qaeda members; it knew they attended a meeting in Malaysia with the mastermind of the USS *Cole* bombing; it even knew that one of the men had entered the United States. Yet the agency resisted telling consular officials at State or intelligence officials at the FBI. Indeed, CIA ignored or flatly denied explicit requests for information about the two men. Hazmi and Mihdhar would go on to help hijack American Airlines Flight 77 and crash it into the Pentagon.

In late 1999, CIA officials learned that an al Qaeda gathering would take place in Kuala Lumpur in January.[45] They also knew, thanks to a tip from an official in Saudi Arabia's intelligence service, that Nawaf al Hazmi and Khaled al Mihdhar—both Saudi citizens—would participate in the meeting.[46] Mihdhar was traveling from Yemen with a stopover in the United Arab Emirates; while he was in Dubai, CIA operatives searched his hotel room.[47] They made a copy of his passport, discovering that the State Department had issued him a multiple-entry visa.[48] That was a strong indication that al Qaeda members were interested in traveling to the United States, and that they may already have done so. Realizing the significance of its discovery, CIA immediately sent an alert to other nations' intelligence services.[49] "The same cable said that the FBI had been alerted to the Malaysia meeting and that the bureau had been given copies of Mihdhar's travel documents. That turned out not to be true."[50]

Back in the States, an FBI agent detailed to the CIA Counterterrorism Center came across the cable and asked for permission to share

---

44 The following account draws heavily from 9/11 COMMISSION REPORT, *supra* note 2; STEVE COLL, GHOST WARS (2004); and LAWRENCE WRIGHT, THE LOOMING TOWER: AL-QAEDA AND THE ROAD TO 9/11 (2007).

45 COLL, *supra* note 44, at 484; WRIGHT, *supra* note 44, at 351–52.

46 COLL, *supra* note 44, at 484; WRIGHT, *supra* note 44, at 351–52.

47 WRIGHT, *supra* note 44, at 351.

48 COLL, *supra* note 44, at 484; WRIGHT, *supra* note 44, at 351.

49 WRIGHT, *supra* note 44, at 351.

50 *Id.*; *see also* COLL, *supra* note 44, at 484. *But see* 9/11 COMMISSION REPORT, *supra* note 2, at 181 (reporting that information about the Malaysia meeting "had been passed on to [National Security Advisor Sandy] Berger and the NSC staff and to Director [Louis] Freeh and others at the FBI (though the FBI noted that the CIA had the lead and would let the FBI know if a domestic angle arose)").

it with his colleagues at the bureau.[51] His hosts said no. "'This is not a matter for the FBI,'" he was told.[52] A week later, the agent renewed his request, this time asking a CIA official who had been detailed to FBI headquarters. "'Is this a no go or should I remake it in some way?' [CIA] never responded. After that, [the FBI agent] forgot about the matter."[53] The diplomats fared no better than the cops. "Nor did the agency notify the State Department to put Mihdhar's name on a terror watch list so that he would be stopped or placed under surveillance if he entered the United States."[54]

Information sharing did not improve as the investigation wore on in subsequent months. On January 8, 2000, Mihdhar and Hazmi flew from Kuala Lumpur to Bangkok, where their trail went cold.[55] Hazmi would take a United Airlines flight to Los Angeles a week later, on January 15, but CIA didn't learn of this for another three months.[56] When CIA found out about Hazmi's arrival, it remained tight-lipped. "The agency neglected to inform either the FBI or the State Department that at least one known al-Qaeda operative was in the country."[57] (If officials had inspected the passenger manifest, they would have seen that Mihdhar was on the same flight.[58])

Fast forward to January 2001. After the USS *Cole* was bombed in Aden harbor on October 12, 2000, Yemeni officials captured an al Qaeda member who was supposed to have videotaped the attack.[59] (He didn't because he overslept.[60]) Under interrogation, the cameraman fingered a man named "Khallad" as the architect of the attack, described him as a close associate of Osama bin Laden, and mentioned that he had delivered money to Khallad in Bangkok.[61] The name rang a bell with an FBI agent who was reviewing the interrogation transcripts. He arranged for a photograph of the person he sus-

---

51 WRIGHT, *supra* note 44, at 351–52.

52 *Id.* at 352.

53 *Id.*

54 *Id.*

55 *Id.*; *see also* 9/11 COMMISSION REPORT, *supra* note 2, at 181.

56 WRIGHT, *supra* note 44, at 352; *see also* 9/11 COMMISSION REPORT, *supra* note 2, at 181.

57 WRIGHT, *supra* note 44, at 352; *see also* 9/11 COMMISSION REPORT, *supra* note 2, at 181–82 (indicating that "CIA did not try to register Mihdhar or Hazmi with the State Department's TIPOFF watchlist—either in January, when word arrived of Mihdhar's visa, or in March, when word came that Hazmi, too had had a U.S. visa and a ticket to Los Angeles," and that "[n]one of this information—about Mihdhar's U.S. visa or Hazmi's travel to the United States—went to the FBI"); COLL, *supra* note 44, at 484–85.

58 WRIGHT, *supra* note 44, at 352.

59 *Id.* at 371.

60 *Id.* at 361.

61 *Id.* at 371.

pected of orchestrating the *Cole* bombing to be shown to the cameraman; the cameraman confirmed that the man in the picture was Khallad.[62] "That was the first real link between the *Cole* bombing and al-Qaeda."[63] His curiosity aroused, the FBI agent then "sent Khallad's photo to the CIA asking for information about him and whether there might have been an al-Qaeda meeting in the region. The agency did not respond to his clearly stated request."[64] The FBI agent sent another message a few days later. "Again, the agency had nothing to say."[65]

Eventually, the FBI's criminal investigators did find out about the Malaysia gathering, its link to the *Cole* attack, and the fact that two of the meeting's participants were in the United States. But it happened almost by accident. By summer 2001—"the summer of threat"[66]—CIA had begun to share information with FBI intelligence analysts,[67] though perhaps not to optimal levels. (Intelligence agencies may have special incentives to share during times of crisis in ways they ordinarily would not.[68]) In late August, Dina Corsi—an intelligence official at FBI headquarters—e-mailed a group of intelligence operatives directing them to investigate whether or not Khaled al Mihdhar was still in the country.[69] She inadvertently copied Steve Bongardt, an FBI agent who was working the criminal investigation of the *Cole* bombing.[70] Bongardt immediately called Corsi with a demand for more information about Mihdhar.[71] She refused, and asked him to delete the message he had received.[72] Bongardt then fired off an angry e-mail: "Whatever has happened to this—someday somebody will die—and wall or not—the public will not understand why we are not more effective and throwing every resource we had at certain 'problems.'"[73]

3. *Other Missteps*

The wall and the summer of threat are fairly spectacular sharing failures. Sometimes failures come not with a bang but a whimper.

---

62 *Id.* at 371–72.

63 *Id.* at 372.

64 *Id.*

65 *Id.* at 373.

66 9/11 COMMISSION REPORT, *supra* note 2, at 254.

67 WRIGHT, *supra* note 44, at 383–86, 398–400.

68 *See infra* note 261.

69 WRIGHT, *supra* note 44, at 398.

70 *Id.* at 399.

71 *Id.*

72 9/11 COMMISSION REPORT, *supra* note 2, at 270.

73 *Id.* at 271.

Consider the federal government's policy on sharing information obtained from foreign governments, adopted by an interagency working group in late 2006. On December 16, 2005, President George W. Bush issued guidelines to improve the flow of information among entities with national security responsibilities.[74] The directive declared that "[e]nsuring the appropriate access to, and the sharing, integration, and use of, information by Federal, State, local, and tribal agencies . . . remains a high priority for the United States and a necessity for winning the war on terror."[75] A handful of agencies—the Office of the Director of National Intelligence, as well as the Departments of Commerce, Defense, Homeland Security, Justice, State, and the Treasury—were then directed to prepare "recommendations for appropriate legislative, administrative, and policy changes to facilitate the sharing of terrorism information with foreign partners and allies."[76] So far so good.

The problem is that the working group's recommendations embrace fairly severe restrictions on information sharing. In particular, one of the group's reports—known in the trade as the "Guideline 4 report"—states that "[i]t may be necessary, as a practical matter, to be willing to accept some [sharing or use] limitations as a condition of receiving information from foreign governments."[77] (These restrictions are known as ORCON, or "originator controls."[78]) According to the report, federal law does not bar such limits; the policy reflected in the Intelligence Reform and Terrorism Prevention Act (which establishes an "information sharing environment"[79]) and Executive Order 13388 (which directs agencies to share terrorism information with one

---

74 *See* Memorandum on Guidelines and Requirements in Support of the Information Sharing Environment: Memorandum for the Heads of Executive Departments and Agencies, 41 WEEKLY COMP. PRES. DOC. 1874, 1874 (Dec. 16, 2005) [hereinafter ISE Guidelines]. For further discussion, see *infra* notes 144–48 and accompanying text.

75 ISE Guidelines, *supra* note 74, at 1874.

76 *Id.* at 1877.

77 INFORMATION SHARING ENVIRONMENT, GUIDELINE 4—FACILITATE INFORMATION SHARING BETWEEN EXECUTIVE DEPARTMENTS AND AGENCIES AND FOREIGN PARTNERS 8, *available at* http://www.ise.gov/pages/documents.aspx [hereinafter GUIDELINE 4 REPORT]. In fairness, the report does allow that "some restrictions are unacceptable, such that the United States would forgo receiving the information or entering into an information sharing agreement, rather than agree to the restrictions." *Id.* But it offers no guidance on how to tell the unacceptable from the acceptable. The inevitable result is that whether a proposed restriction is acceptable will depend on whether the agency that is considering it determines that it will help or hinder its own parochial interests.

78 See MARK M. LOWENTHAL, INTELLIGENCE: FROM SECRETS TO POLICY 154 (4th ed. 2009).

79 *See infra* notes 124–34 and accompanying text.

another[80]) "is consistent" with such arrangements.[81] The effect of the Guideline 4 report is to greenlight individual agencies that negotiate with foreign counterparts to accept (and maybe even propose?) limits on their ability to share foreign information with other federal agencies. The members of the working group effectively made a pact in which each agreed not to demand access to one another's foreign-source information in exchange for immunity from the same requests by other agencies.

A second, lesser-noticed sharing failure concerns the standards for exchanging "sensitive but unclassified information," also known as "controlled unclassified information" or "CUI."[82] CUI is not classified, but the government nevertheless believes the data to be sufficiently sensitive that its public release could harm national security.[83] Examples include data about ongoing criminal investigations (the release of which could alert suspects that they have been compromised) and vulnerabilities at chemical plants (which terrorists could exploit to plan attacks). Historically, there have been dozens of different classes of CUI, such as "law enforcement sensitive"[84] and "chemical vulnerability information."[85] With nearly 60 different CUI categories,[86] it was probably inevitable that confusion would arise about whether the data could be shared at all, with whom, and under what conditions it was to be stored. And so it did. A March 2006 Government Accountability Office report found that "[t]here are no governmentwide policies or procedures that describe the basis on which agencies should use most of these sensitive but unclassified designations, explain what the different designations mean across agencies, or ensure that they will be used consistently from one agency to another."[87] As a result, "[m]ore than half of the agencies reported encountering challenges in sharing such information."[88] In response, President Bush issued a directive on

---

80 *See infra* notes 140–43 and accompanying text.

81 GUIDELINE 4 REPORT, *supra* note 77, at 10.

82 *See* Memorandum on Designation and Sharing of Controlled Unclassified Information (CUI), 44 WEEKLY COMP. PRES. DOC. 673, 673 (May 7, 2008) [hereinafter CUI Designation Memo].

83 *See id.* at 673–74.

84 *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-06-385, REPORT TO CONGRESSIONAL REQUESTERS, INFORMATION SHARING: THE FEDERAL GOVERNMENT NEEDS TO ESTABLISH POLICIES AND PROCESSES FOR SHARING TERRORISM-RELATED AND SENSITIVE BUT UNCLASSIFIED INFORMATION 22 (2006) [hereinafter GAO, INFORMATION SHARING].

85 CUI Designation Memo, *supra* note 82, at 677.

86 *See* GAO, INFORMATION SHARING, *supra* note 84, at 22–23.

87 *Id.* at 5.

88 *Id.*

May 7, 2008, instructing all executive branch agencies to adopt common CUI rules.[89] In particular, agencies are to use a uniform set of dissemination markings that specify with whom and under what circumstances a given document may be shared.[90] The directive also orders agencies to use common handling markings, which indicate the conditions under which recipients of the document must store it.[91] The idea is to sweep away legacy rules on how various types of CUI are shared and stored, and replace them with uniform standards that (it is hoped) will facilitate sharing.

The new CUI regime contains several exceptions. Four categories of data are exempt from the new rules and will continue to be shared—or not shared, as the case may be—according to the old standards.[92] They are: "Protected Critical Infrastructure Information" (data about critical infrastructure, such as railways and Internet backbone[93]), "Sensitive Security Information" (information about the screening of airline passengers, baggage, and cargo[94]), "Chemical Vulnerability Information" (information about chemical-plant facilities, processes, and security plans[95]), and "Safeguards Information" (data about nuclear power plants and materials[96]). The Department of Homeland Security ("DHS") controls each type of information; in most cases, DHS acquires the data when private firms voluntarily turn it over to the agency.[97] The effect of the CUI exemptions is that DHS is under no obligation to share those categories of information. Why would the President exempt data from the new sharing regime? The most likely answer is that he was successfully lobbied to do so by the custodian agency—DHS.

A final example comes from 2001. FBI officials and the U.S. Attorney's office in the Southern District of New York were responsible for investigating and prosecuting a number of al Qaeda attacks, including the 1998 embassy bombings and the 2000 strike on the USS

---

89 *See* CUI Designation Memo, *supra* note 82, at 673.

90 *See id.* at 674–75.

91 *See id.* at 673–74.

92 *See id.* at 677.

93 *See* 6 C.F.R. pt. 29 (2009).

94 *See* 49 C.F.R. § 1520.5 (2009).

95 *See* 6 C.F.R. § 27.400 (2009).

96 *See* 10 C.F.R. § 73.22 (2009).

97 *See, e.g.*, U.S. Dep't of Homeland Sec., Protected Critical Infrastructure Information (PCII) Program, http://www.dhs.gov/files/programs/editorial_0404.shtm (describing the PCII as "an information-protection program that enhances information sharing between the private sector and the government").

Cole.[98] Naturally, they wanted access to National Security Agency ("NSA") intercepts of Osama bin Laden's satellite telephone calls.[99] Initially the NSA was willing to share the intercepts but later began to withhold them, evidently to protect the agency's sensitive intelligence sources and methods.[100] As a workaround, the Justice Department team "came up with a plan to build two antennae, one in the remote Pacific islands of Palau and another in Diego Garcia, in the Indian Ocean, that would capture the signal from the satellite"; they also "constructed an ingenious satellite telephone booth in Kandahar for international calls, hoping to provide a convenient facility for jihadis wanting to call home."[101] Faced with the bureau's determination to collect the intelligence on its own, the NSA eventually relented and handed over the intercepts.[102]

B. Post-9/11 Information-Sharing Initiatives

Policymakers in Congress and the executive branch have adopted a number of measures to cure these and other perceived problems with information sharing since the 9/11 terrorist attacks. These initiatives reflect diverse—and, at times, contradictory—policy visions. Some measures do no more than eliminate legal restrictions on information sharing. Others more ambitiously, if unsuccessfully, set about to foster an interagency culture that prizes data exchange. Some reforms envision a centralized clearinghouse of all intelligence information under the control of a single officer. Others reflect a preference for decentralization, in which data is stored at various nodes within a distributed network.

The federal government's first major post-9/11 information-sharing initiative was the inelegantly named USA PATRIOT Act.[103] That

---

98 *See* WRIGHT, *supra* note 44, at 382–88.

99 *See id.* at 388.

100 *See id.* at 387–88.

101 *See id.* at 388.

102 *See id.*

103 The original name for the Bush Administration proposal was the "Mobilization Against Terrorism Act," or MATA—not coincidentally, a derivative of "matar," the Spanish word for "to kill." *See* Press Release, U.S. Dep't of Justice, Attorney General Ashcroft Outlines Mobilization Against Terrorism Act (Sept. 24, 2001), http://www.usdoj.gov/archive/opa/pr/2001/September/492ag.htm. When that was deemed too bellicose, the Administration rechristened its legislative package with the rather more saccharine moniker "Anti-Terrorism Act." But some in Congress fretted that the acronym ATA was too reminiscent of "Atta," the surname of one of the 9/11 hijackers. *See* Beryl A. Howell, *Seven Weeks: The Making of the USA PATRIOT Act*, 72 GEO. WASH. L. REV. 1145, 1153 n.43 (2004). So the Senate and the House of Representatives picked new names. The Senate bill was dubbed the "Uniting and Strengthening America Act," while its

legislation eliminated a number of legal barriers that had prevented law-enforcement personnel from sharing information they uncovered in the course of criminal investigations with their counterparts in the intelligence community. For instance, section 203 amended Federal Rule of Criminal Procedure 6(e),[104] which generally bars attorneys for the government from "disclos[ing] a matter occurring before the grand jury."[105] After the PATRIOT Act, investigators may share grand-jury information that "involve[s] foreign intelligence or counterintelligence . . . or foreign intelligence information" with "any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official."[106] They need not obtain a judge's approval before doing so. Section 203 made similar changes to the federal wiretap statute,[107] which was read to restrict law-enforcement officers to sharing the fruits of electronic surveillance with other criminal investigators.[108] The PATRIOT Act removed that limitation, authorizing cops to share intercepts with spies "to the extent that such contents include foreign intelligence or counterintelligence . . . or foreign intelligence information."[109] In addition to this pair of belts, Congress donned a set of suspenders. Section 905 broadly directs the Attorney General to "expeditiously disclose to the Director of Central Intelligence . . . foreign intelligence acquired by an element of the Department of Justice . . . in the course of a criminal investigation."[110]

The PATRIOT Act promoted the flow of information in the opposite direction, as well—from intelligence analysts to law-enforcement officers. As discussed above,[111] the Justice Department had

---

House counterpart was the even more imaginative "Provide Appropriate Tools Required to Intercept and Obstruct Terrorism." *See id.* at 1155, 1172. Congressional leaders couldn't decide which they liked better, so they used both. The result of this determined acronyming was the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001," Pub. L. No. 107-56, 115 Stat. 272. *See* Howell, *supra*, at 1174–77.

104 USA PATRIOT Act § 203(a), 115 Stat. at 278–81 (amending FED. R. CRIM. P. 6(e)).

105 *See* FED. R. CRIM. P. 6(e)(2)(B); *see also* COLL, *supra* note 44, at 255.

106 USA PATRIOT Act § 203(a)(1), 115 Stat. at 279 (codified at FED. R. CRIM. P. 6(e)(3)(C)(i)(V)). Academics disagree about whether these changes to the grand-jury rules are justified. *Compare* Lerner, *supra* note 1, at 520–25 (sharing appropriate), *with* Collins, *supra* note 3, at 1270–86 (sharing appropriate, but only with prior judicial approval).

107 USA PATRIOT Act § 203(b), 115 Stat. at 280 (codified at 18 U.S.C. §§ 2510, 2517 (2006)).

108 *See generally* 18 U.S.C. § 2517 (2000).

109 USA PATRIOT Act § 203(b)(1), 115 Stat. at 280 (codified at 18 U.S.C. § 2517(6) (2006)).

110 *Id.* § 905(a)(2), 115 Stat. at 389 (codified at 50 U.S.C. § 403-5b (2006)).

111 *See supra* notes 14–43 and accompanying text.

erected a "wall" isolating the FBI's intelligence analysts from officials responsible for investigating ordinary crimes. Sections 218 and 504 abolished that wall. Under the former, it's no longer necessary for the government to certify to the FISA court that "the primary purpose" of proposed surveillance is to gather foreign intelligence. Now, investigators may use FISA whenever foreign intelligence is "a significant purpose" of the surveillance.[112] Section 504 is even more explicit. It provides that intelligence officials "may consult with Federal law enforcement officers to coordinate efforts" against national security threats.[113] In 2002, the Foreign Intelligence Surveillance Court of Review (a specialized appellate court established by FISA) upheld these provisions (and the Justice Department's procedures to implement them) against Fourth Amendment and other challenges.[114] As a result, the FBI's intelligence officials now have a freer hand to share information with criminal investigators; prosecutors also are able to play a more active role in overseeing intelligence investigations and deciding what information should be shared.

The USA PATRIOT Act is often hailed for tearing down the wall that kept intelligence and criminal officials from cooperating with one another. For instance, Judge Posner argues that the Act "accomplished" the goal of "eliminating artificial barriers to the pooling of intelligence data."[115] Those plaudits are unwarranted. The PATRIOT Act's information-sharing ambitions are actually quite modest. The Act is largely limited to eliminating various legal rules that had barred officials from exchanging data with one another. It did nothing to give agencies a reason to share once those restrictions were lifted; Congress left the underlying incentive structures untouched. The PATRIOT Act seems to have assumed that, in the absence of legal prohibitions, data would flow freely among members of the intelligence community, and that no additional inducements were needed to persuade agencies to share.

---

112 USA PATRIOT Act § 218, 115 Stat. at 291 (codified at 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B) (2006)).

113 *Id.* § 504, 115 Stat. at 364–65 (codified at 50 U.S.C. §§ 1806(k), 1825(k) (2006)).

114 *In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002). Academic opinion is split on section 218 and the FISCR's decision. *Compare* Banks, *supra* note 3, at 1171–84 (accepting the need for more sharing but criticizing the expanded role for prosecutors in directing intelligence investigations), *with* Kris, *supra* note 1, at 518–28 (defending section 218 and the FISCR's decision), *and* Paul Rosenzweig, *Civil Liberty and the Response to Terrorism*, 42 DUQ. L. REV. 663, 686–91 (2004) (same), *and with* Seamon & Gardner, *supra* note 1, at 455–58 (faulting the FISCR for adopting an unduly restrictive interpretation of section 218, and arguing that the government may use FISA surveillance even if its sole purpose is to collect evidence for use in prosecution).

115 POSNER, SURPRISE ATTACKS, *supra* note 1, at 122.

The Homeland Security Act of 2002[116] reflects a more jaundiced view of agency behavior. The Act cobbled together a new Department of Homeland Security from 22 different components drawn from legacy agencies.[117] Section 892 is its major contribution to information-sharing policy. That provision directs that, "[u]nder procedures prescribed by the President, all appropriate agencies, including the intelligence community, shall, through information sharing systems, share homeland security information with Federal agencies and appropriate State and local personnel."[118] Unlike the PATRIOT Act, Congress did not just make it legally permissible for agencies to share information. It imposed an affirmative obligation to do so ("all appropriate agencies . . . shall . . . share"). Notice also that section 892 reflects a congressional commitment to decentralization. No single intelligence official is given custody of the federal government's entire catalogue of counterterrorism information; instead, the data is housed at various points throughout the intelligence system.[119]

The Homeland Security Act contains another, lesser-noticed information-sharing provision. Section 202 grants the Secretary of Homeland Security "such access as the Secretary considers necessary to all information . . . relating to threats of terrorism against the United States . . . that may be collected, possessed, or prepared by any agency of the Federal Government," as well as "other information relating to matters under the responsibility of the Secretary."[120] Section 202 envisions three ways DHS might acquire terrorism-related information: "upon request" of the Secretary, pursuant to "cooperative arrangements" that provide for "regular or routine" access, and at the initiative of other agencies.[121] In other words, DHS can demand that another agency give it a discrete piece of information in which it has a particular interest ("retail" sharing). It can enter an agreement by which another agency pledges routinely to share large troves of data that might, as a class, be useful to DHS's counterterrorism mission

---

116 Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (codified as amended in scattered sections of 6 U.S.C.).

117 *See* POSNER, UNCERTAIN SHIELD, *supra* note 7, at 125.

118 Homeland Security Act § 892(b)(1), 116 Stat. at 2253 (codified at 6 U.S.C. § 482(b)(1) (2006)). The President delegated to the Secretary of Homeland Security his responsibility for establishing the procedures contemplated by section 892. *See* Exec. Order No. 13,311, 68 Fed. Reg. 45,149 (July 29, 2003).

119 *See* Homeland Security Act § 892(d), 116 Stat. at 2255 (codified at 6 U.S.C § 482(d) (2006)) (requiring the head of "each affected Federal agency" to "designate an official to administer" the information sharing contemplated by the Act).

120 *Id.* § 202(a)(1)–(2), 116 Stat. at 2149 (codified at 6 U.S.C. § 122(a)(1)–(2) (2006)).

121 *Id.* § 202(b)(1)–(2), 116 Stat. at 2149–50 (codified at 6 U.S.C. § 122(b)(1)–(2) (2006)).

("wholesale" sharing). Or another agency can take the initiative and volunteer information about which DHS might not be aware but which the agency believes would be of interest ("volunteer" sharing). These mechanisms embody a centralized approach to information sharing—an "inverted-V pattern" arrangement.[122] A single regulator is given authority to gather and warehouse all of the federal government's terrorism information, which it then hands out to other agencies.[123]

The Homeland Security Act thus reflects a dawning congressional realization that effective information sharing depends on arm twisting. Gone is PATRIOT's assumption that abolishing legal restrictions, without more, will ensure the free flow of data. Instead, Congress saw the need to compel agencies to share: it established that agencies have an affirmative obligation to share, and it granted the Secretary of Homeland Security new powers to demand data. This represents a welcome refinement in Congress's thinking about how to make data exchange a reality, but the Act has its limits. While Congress imposed duties on agencies to share information—both with each other and with DHS—it did not specify any consequences for failing to do so. Nor did Congress create a mechanism to enforce its new sharing obligations. The Homeland Security Act is largely hortatory. Because the act lacks teeth, it has little effect on agencies' natural incentives to hoard—if any at all.

Congress's thinking about how to promote information sharing evolved further in the Intelligence Reform and Terrorism Prevention Act of 2004[124] ("IRTPA"). IRTPA's boldest—and most controversial[125]—move was to reorganize the intelligence community by placing it under the oversight of a new "Director of National Intelligence" ("DNI"), who also would serve as the chief intelligence advisor to the

---

122 POSNER, UNCERTAIN SHIELD, *supra* note 7, at 68. Judge Posner objects to a centralized sharing mechanism for efficiency reasons; he worries that forcing data to "flow[ ] up the hierarchy to the decision-making level from one agency and down the hierarchy to another" will "creat[e] delay and a risk of losing or garbling vital information." *Id.*

123 DHS has rarely, if ever, exercised its section 202 powers to demand access to other agencies' information. This is mostly due to changing assumptions about DHS's role within the intelligence community. The Homeland Security Act assumed that DHS would be the federal government's primary clearinghouse for all counterterrorism information, *see* FIRST MARKLE REPORT, *supra* note 2, at 71–72, but today that role is performed by the National Counterterrorism Center.

124 Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638.

125 *See* POSNER, SURPRISE ATTACKS, *supra* note 1, at 51–69 (criticizing creation of Director of National Intelligence).

President.[126] Less ambitiously, section 1016 of the legislation established a new "information sharing environment," or "ISE"—i.e., "an approach that facilitates the sharing of terrorism information, which approach may include any methods determined necessary and appropriate."[127] IRTPA's information-sharing reforms are largely structural, not substantive. The act creates new institutions—e.g., the ISE, the Program Manager responsible for overseeing the ISE,[128] the Information Sharing Council,[129] and so on—but it offers only the barest guidance on what policies those institutions should pursue.[130]

For example, IRTPA calls for the Information Sharing Environment to be "decentralized, distributed, and coordinated."[131] Congress thus opted for an intelligence system in which information is held by a number of different players. This federated model resembles Homeland Security Act section 892 (which broadly directs members of the intelligence community to exchange information with one another),[132] and differs profoundly from the centralized model envisioned by section 202 of that same legislation (under which all information would be held by central clearinghouse).[133] Another of IRTPA's more substantive features is its recognition of the need to appeal to agencies' self-interest: the Act expressly calls on the President to "promote a culture of information sharing by . . . reducing disincentives to information sharing, including over-classification of information and unnecessary requirements for originator approval," as well as by "providing affirmative incentives for information sharing."[134] Unfortunately, IRTPA doesn't contribute much more than general platitudes. The legislation reflects only the thinnest analysis of why it might be in agencies' interests to resist data exchange—i.e., because agencies fear leaks and espionage, and because they want to maintain control over their information. Equally problematic, the Act offers no suggestions whatsoever about how to foster favorable information-

126 Intelligence Reform and Terrorism Prevention Act § 1011(a), 118 Stat. at 3643–61 (codified at 50 U.S.C § 403(a) (2006)).

127 *Id.* § 1016(a)(2), 118 Stat. at 3665 (codified at 6 U.S.C. § 485(a)(2) (2006)).

128 *Id.* § 1016(f), 118 Stat. at 3667–68 (codified at 6 U.S.C. § 485(f) (2006)).

129 *Id.* § 1016(g), 118 Stat. at 3668–69 (codified at 6 U.S.C. § 485(g) (2006)).

130 *See id.* § 1016(b)(1)(C), 118 Stat. at 3665 (codified at 6 U.S.C § 485(b)(1)(C) (2006)) (broadly delegating to the President the authority to "determine and enforce the policies, directives, and rules that will govern the content and usage of the ISE").

131 *Id.* § 1016(b)(2), 118 Stat. at 3665–66 (codified at 6 U.S.C. § 485(b)(2) (2006)).

132 *See supra* notes 118–19 and accompanying text.

133 *See supra* notes 121–22 and accompanying text.

134 Intelligence Reform and Terrorism Prevention Act § 1016(d)(3), 118 Stat. at 3666 (codified at 6 U.S.C. § 485(d)(3) (2006)).

sharing incentives. IRTPA asks the right questions, but it is woefully short on answers.

Not all of the action has been on Capitol Hill; the executive branch has adopted information-sharing reforms of its own. On August 27, 2004, President George W. Bush issued a pair of executive orders intended to promote data exchange. The first, Executive Order 13354, generally directed federal agencies to "give the highest priority to . . . the interchange of terrorism information among agencies."[135] It further created a National Counterterrorism Center ("NCTC") to, among other things, "serve as the primary organization in the United States Government for analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to terrorism and counterterrorism."[136] Just as Homeland Security Act section 202 conceives of DHS, Executive Order 13354 envisions the NCTC as a centralized conduit through which data will flow among the government's various intelligence agencies. NCTC will "receive, retain, and disseminate" terrorism-related information, while "serv[ing] as the central and shared knowledge bank on known and suspected terrorists and international terror groups."[137] For their part, intelligence agencies are to "promptly give access to [terrorism] information to the Director of the Center."[138] They also "may query Center data for any information to assist in their respective responsibilities."[139] Agencies thus are to share information through the NCTC as an intermediary, rather than directly as peers.

What Executive Order 13354 gave, Executive Order 13356 took away. Issued the same day, Executive Order 13356 directed that "the head of each agency that possesses or acquires terrorism information . . . shall promptly give access to the terrorism information to the head of each other agency that has counterterrorism functions."[140] Unlike its twin, this order contemplates a distributed network in which information is held by a number of different agencies. Intelli-

135 Exec. Order No. 13,354 § 1(a), 69 Fed. Reg. 53,589, 53,589 (Sept. 1, 2004).

136 *Id.* § 3(a), 69 Fed. Reg. at 53,589.

137 *Id.* § 3(a), (d), 69 Fed. Reg. at 53,589–90.

138 *Id.* § 6(a)(i)(A), 69 Fed. Reg. at 53,591.

139 *Id.* § 3(a), 69 Fed. Reg. at 53,589; *see also id.* § 3(c), 69 Fed. Reg. at 53,589 ("The Center shall ensure that agencies have access to and receive intelligence needed to accomplish their assigned activities.").

140 Exec. Order No. 13,356 § 2, 69 Fed. Reg. 53,599, 53,599 (Aug. 27, 2004). President Bush later revoked Executive Order 13356, *see* Exec. Order No. 13,388 § 8, 70 Fed. Reg. 62,023, 62,025 (Oct. 27, 2005), but its substantive provisions live on largely unchanged. *Compare* Exec. Order No. 13,356, 69 Fed. Reg. 53,599 (Aug. 27, 2004), *with* Exec. Order No. 13,388, 70 Fed. Reg. 62,023 (Oct. 27, 2005).

gence agencies are to exchange information with one another directly, not route it though a central data broker like the NCTC.[141] Executive Order 13356 resembles IRTPA in an important respect: it recognizes the need to appeal to agencies' interests. Toward that end, the order directs agencies to implement "appropriate arrangements providing incentives for, and holding personnel accountable for, increased sharing of terrorism information."[142] The order also recognizes that otherwise necessary classification rules can serve as impediments to sharing, and directs agencies to create unclassified versions of intelligence assessments whenever possible, to share terrorism information free of originator controls, to minimize the compartmentalization of terrorism information, and so on.[143]

Regrettably, the order also shares some of IRTPA's flaws. It acknowledges the importance of incentives but provides no guidance on what specific steps might be taken to encourage sharing and discourage hoarding. Nor does it contain an enforcement mechanism to translate into practice its calls to limit ORCON and compartmentalization rules. Like so many legislative data-sharing initiatives, Executive Order 13356 is largely hortatory.

In late 2005, President Bush also issued a set of guidelines to govern the Information Sharing Environment established by IRTPA.[144] Among other things, the ISE guidelines direct intelligence agencies to establish common standards; develop procedures for sharing information with state, local, and tribal governments; standardize procedures for data that is sensitive but unclassified; and facilitate sharing with foreign partners.[145] They also takes sides in the dispute between Executive Orders 13354 and 13356, expressing a preference for the latter's federated information network: "The ISE shall . . . establish[ ] a decentralized, comprehensive, and coordinated environment for the sharing and integration of such information."[146] The most important feature of the guidelines comes at the end:

> Heads of executive departments and agencies must actively work to create a culture of information sharing within their respective departments or agencies by assigning personnel and dedicating resources to terrorism information sharing,

---

141 Exec. Order No. 13,356, 69 Fed. Reg. at 53,599–600

142 *Id.* § 3(e), 69 Fed. Reg. at 53,600.

143 *Id.* § 3(a), (c), (d), 69 Fed. Reg. at 53,599–600.

144 *See* ISE Guidelines, *supra* note 74. For additional discussion of the guidelines, see *supra* notes 74–81 and accompanying text.

145 *See* ISE Guidelines, *supra* note 74, at 1876–77.

146 *Id.* at 1874–75.

> by reducing disincentives to such sharing, and by holding their senior managers and officials accountable for improved and increased sharing of such information.[147]

So far this is familiar terrain. Yet, unlike previous legislative and executive efforts, the ISE guidelines do more than simply recite the importance of appealing to agencies' interests. They also direct a number of specific steps on how to do so. To wit, agencies are to "provide accountability and oversight for terrorism information sharing"; "develop high level information sharing performance measures"; prepare "an annual report" on "best practices of and remaining barriers to optimal terrorism information sharing"; "provide training and incentives" to employees with information-sharing responsibilities; and "hold relevant personnel accountable" for sharing data, including by "add[ing] a performance evaluation element" to their annual performance reviews.[148] The ISE guidelines seek to mitigate existing incentives to hoard, and for that reason they are perhaps the most promising of the federal government's post-9/11 sharing initiatives.

II. Why Don't Intelligence Agencies Share Information?

The tendency of intelligence agencies to hoard information is ultimately a problem of agency costs—in particular, the costs principals incur when their agents have interests that diverge from their own.[149] As we saw in Part I, the federal government's principals (Congress and the President) have, through a series of legislation and directives, instructed their agents (members of the intelligence community) to share information with one another. Yet the agencies resist implementing those commands. The reason is that their interests differ from those of their principals. Policymakers have an interest in sharing; more data exchange results in improved intelligence assessments,[150] which in turn enables principals to make better decisions. But intelligence agencies have an interest in hoarding.[151] This Part

---

147 *Id.* at 1878.

148 *Id.*

149 *Cf.* Stephanos Bibas, *Prosecutorial Regulation Versus Prosecutorial Accountability*, 157 U. PA. L. REV. 959 (2009) (using a principal-agent framework to explain prosecutor accountability to the general public, victims, and other stakeholders).

150 *See, e.g.*, J. Roderick MacArthur Found. v. FBI, 102 F.3d 600, 604 (D.C. Cir. 1996) ("[I]ntelligence gathering is 'akin to the construction of a mosaic,' to appreciate the full import of a single piece may require the agency to take a broad view of the whole work." (quoting *In re* United States, 872 F.2d 472, 475 (D.C. Cir. 1989))). *See generally* David E. Pozen, Note, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628 (2005).

151 *See* POSNER, SURPRISE ATTACKS, *supra* note 1, at 43 ("[T]he different intelligence ser-

tries to explain why. The first Section considers what intelligence agencies maximize and offers some preliminary observations on how information sharing can undermine those goods. The next three Sections elaborate on the theme. Each proposes a different analytical "lens" through which the hoarding problem might be viewed. Sometimes, agency reluctance to share resembles an intellectual-property problem. Sometimes it looks like an antitrust problem. And sometimes it resembles a problem of organizational culture.

A. What Do Intelligence Agencies Maximize?

It might be helpful to think of the intelligence-production cycle in private-sector terms.[152] Like a private firm, an intelligence agency purchases certain inputs—"raw" or "unprocessed" information. The agency uses its various sources and methods to collect these bits of data (for example, an intercepted e-mail, a report from a covert operative overseas, etc.). The next step is to prepare these inputs for analysis by subjecting them to initial "processing and exploitation," such as decryption or translation. Then the information is handed over to analysts, who complete the production cycle by using their creative energies to interpret, synthesize, and integrate the data into a finished intelligence assessment. The resulting outputs offer warnings of possible threats to the national security, insights into the possible intentions and capabilities of foreign powers, assessments of vulnerabilities in America's defenses, and so on. The agency sells these products to intelligence consumers. The consumers are senior executive branch policymakers—the President and his national security team at the White House, as well as senior agency officials with national security responsibilities, such as the Attorney General, Secretary of Defense, and Director of National Intelligence. Consumers then use the intelligence products they have purchased to inform their deliberations and decisionmaking.[153]

---

vices . . . tend, because information is power, to hoard it."); Anne Joseph O'Connell, *The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post-9/11 World*, 94 CAL. L. REV. 1655, 1681 (2006) (indicating that rival intelligence agencies "may hide their data from their competitors").

152 *See generally* LOWENTHAL, *supra* note 78, at 55–67 (summarizing the intelligence-production cycle).

153 I am analogizing the intelligence community to a group of discrete firms that vie against one another to sell products to executive branch consumers. An alternative is to think of the intelligence community as separate units within a single firm headed by those same policymakers. Just as Pepsi and Frito-Lay are separate divisions of one corporate entity (PepsiCo), so too the FBI, CIA, and other intelligence agencies are subunits of a single enterprise (the intelligence community, or maybe more broadly the executive branch as a whole), of which the President is

Some caveats are needed. The behavior of public agencies often resembles the behavior of private firms but they are not on all fours.[154] One obvious difference is that an agency's sale of finished intelligence product to a senior policymaker is not a neat and tidy transaction akin to the trade of cash for a good. The agency is compensated in the form of future budgetary outlays,[155] but its compensation package also contains a large (and maybe even predominant) nonpecuniary element. An agency that sells intelligence also receives income in the form of enhanced prestige and, derivatively, influence and autonomy. The more prestigious an agency is, the more likely policymakers are to listen to it, and the more success it likely will have at fending off rivals' encroachments on its turf.[156] (More about influence and autonomy in a moment.)

Another complication is that the intelligence product and compensation (monetary and otherwise) don't change hands simultaneously. Instead, the complex transaction unfolds over the course of many months, often many years. An intelligence agency receives something like deferred compensation. The better its products vis-à-vis those of rival agencies, the more likely senior officials are to rely on the agency's judgment (and the more money future budgets are likely to route to the agency). Conversely, the worse the agency's products are compared to competitors', the less influence it will wield in the future (and the less likely it is to receive generous budgetary outlays). But those gains and losses aren't realized for a long time. In addition, the compensation an agency receives usually cannot be traced to individual intelligence assessments. Instead, it typically reflects a rolling assessment of the value of the agency's analytical out-

---

the CEO. The "separate firms" analogy seems more apt because of the complex role played by the President. It's true that agencies are subordinate to the President and other policymakers just as business units are subordinate to corporate executives. But agencies and the President also relate to one another as producers and consumer. Because the intelligence community is not just a hierarchical system—i.e., because the President functions both as an agency's superior and as a consumer of its goods—it makes more sense to think of the system as comprising separate, rival firms.

154 *See* POSNER, SURPRISE ATTACKS, *supra* note 1, at 105. *See generally* JAMES Q. WILSON, BUREAUCRACY xviii (2d ed. 2000); ZEGART, *supra* note 38, at 54–56.

155 *See* LOWENTHAL, *supra* note 78, at 216; WILLIAM A. NISKANEN, JR., BUREAUCRACY AND REPRESENTATIVE GOVERNMENT 38–39 (1971).

156 The more prestige income an agency receives today, the more likely it is that senior policymakers will buy more of its products tomorrow (and the less likely it is they will purchase outputs from the agency's rivals). This is similar to the private-sector concept of business goodwill. If consumers are pleased with the quality of the goods or services they have bought from a producer, they are more likely to return for more goods or services in the future.

puts over a period of time.[157] That longer time horizon between the sale of an item and the receipt of compensation complicates any efforts to use private-sector incentives and mechanisms to influence the behavior of administrative agencies.[158]

Finally, it's notoriously difficult to measure the value of agency outputs. "Of all such commodities produced by government, intelligence is one of the hardest to value."[159] Output valuation typically is not a problem in the private sector; the value of a firm's widget is equal to the price it commands in a sale on the open market, and a firm's overall performance can be judged pretty effectively by looking at its annual profits. But agency outputs are usually informational, not tangible, and there is no open market in which intelligence products (whether raw or finished) may be bought and sold. An agency can never be completely sure of the "real" value of the informational inputs it buys, nor of the finished informational outputs it sells. These valuation difficulties—and the resulting atmosphere of uncertainty—have important implications for the willingness of rival agencies to exchange information with one another.

A simplistic "agency = firm" analogy won't do, but the private-sector model has enough explanatory power that it is a useful framework through which to understand the behavior of intelligence agencies. Private firms maximize profits; what do agencies maximize? A broad inquiry into the utility functions of administrative agencies as such is beyond the scope of this article.[160] But intelligence agencies in

---

157 *See* LOWENTHAL, *supra* note 78, at 216–17

158 A related problem is that the President does not determine intelligence agencies' budgets unilaterally. His Administration submits proposals to Congress, which the legislature is free to modify as it sees fit. *See* POSNER, SURPRISE ATTACKS, *supra* note 1, at 38. The President proposes and Congress disposes. This congressional role further complicates the links between agency budgets and performance. Members of Congress might adjust an agency's budget for reasons that have little to do with the quality of its products. For example, a member might slash a proposed budget because the agency has resisted congressional oversight, or a member might augment a proposed budget because the agency's headquarters are located in the member's district. In other words, intelligence agencies' budgets reflect the relative quality of their products, but they also reflect unrelated factors such as the extent of their cooperation with Congress and the influence of their congressional patrons.

159 POSNER, SURPRISE ATTACKS, *supra* note 1, at 105; *see also* LOWENTHAL, *supra* note 78, at 216.

160 *See, e.g.*, Levinson, *supra* note 8, at 920 (explaining that government officials' interests include "effectuating their preferred policies, contributing to the success of their political party, seeking greater personal influence within their institution, and angling for higher office"); NISKANEN, *supra* note 155, at 38 (indicating that bureaucrats generally pursue "salary, perquisites of the office, public reputation, power, patronage, output of the bureau, ease of making changes, and ease of managing the bureau").

particular appear to seek at least two things. First, intelligence agencies seek influence, by which is meant the ability to mold the decisions of the senior policymakers who consume the agency's intelligence products (and the ability to prevent rival agencies from doing the same). Second, agencies seek autonomy, by which is meant the ability to pursue their core priorities without external interference.[161] Intelligence agencies have strong incentives to hoard, because sharing can undermine both goods. The result is negative externalities. An agency that hoards captures all the benefits—namely, enhanced influence and autonomy. But the costs are borne by others—rival agencies are denied potentially useful data, which in turn means lower quality intelligence products are available to executive branch decisionmakers.

Consider influence first. An intelligence agency wants to maximize the sway it holds over senior policymakers in the executive branch—i.e., White House officials up to (and especially) the President. By influence I mean that the agency is able to persuade its superiors to share its judgments about possible threats against the United States, the intentions and capabilities of hostile foreign powers, and vulnerabilities in American defenses, and that policymakers choose a course of action other than one they would have chosen in the absence of the agency's intelligence assessment. At the same time, agencies want to minimize the influence rival agencies have over senior policymakers. CIA wants the President to believe its assessment that a given Algeria-based terrorist cell poses only a modest threat to the national security, not the NSA's assessment that the threat is grave indeed.

There is some anecdotal evidence that intelligence agencies do indeed seek to maximize their influence over White House policymakers. Consider the Presidential Daily Brief ("PDB"), a digest of intelligence analyses that the Director of National Intelligence provides to

---

161 Notice that budgets aren't on the list. *Contra* NISKANEN, *supra* note 155, at 38–39; William A. Niskanen, Jr., *Bureaucrats and Politicians*, 18 J.L. & ECON. 617, 618–19 (1975) (arguing that agencies seek to maximize their discretionary budgets—i.e., "the difference between . . . total budget and the minimum cost of producing the expected output"—as opposed to their budgets more generally). Often agencies do seek larger budgets (i.e., when doing so would enhance an agency's ability to achieve its priorities). But sometimes they resist external efforts to expand their budgets (i.e., when the associated new responsibilities would distract an agency from its core priorities, undermine its prestige, or otherwise harm its autonomy). *See infra* notes 175–83 and accompanying text. In other words, what looks like budget maximization in reality is often autonomy maximization. *Cf.* WILSON, *supra* note 154, at xvii (arguing that "bureaucrats have a variety of preferences; only part of their behavior can be explained by assuming they are struggling to get bigger salaries or fancier offices or larger budgets").

the President every morning.[162] It is considered a crowning achievement within the intelligence community for an analyst to have one of his reports included in the PDB.[163] (This creates incentives that distort intelligence analysis. The items that make it into the PDB are the ones with the gripping headline summaries.[164] Analysts thus will tend to overstate conclusions that are in fact tentative, and resist caveating their conclusions by pointing to contrary evidence.[165]) Agencies themselves are subject to the same pressures, and they therefore try to maximize their number of entries in the PDB as a way of gaining influence over the President. Also, since the number of PDB entries is finite, they try to crowd out assessments from rival agencies that otherwise might have been included.[166]

Another piece of anecdotal evidence that agencies seek to maximize their influence is their occasional tendency to provide executive branch decisionmakers with assessments that reinforce the officials' preconceptions. Agencies sometimes act like yes-men. Here, the measure of influence is somewhat different: instead of persuading the policymaker to take a different course than he otherwise would have, the agency provides further justification for the course the policymaker has already settled on.[167] Some believe that this yes-man effect was present in the run-up to the 2003 Iraq war. That is, Administration officials heeded agency warnings that Saddam Hussein's Iraq had and was seeking weapons of mass destruction, and disregarded evidence to the contrary.[168] The effect on agency behavior was fairly predictable. Agencies started preparing custom-fit intelligence assessments—their analyses came to reflect the preconceived notions held by their consumers.[169]

How does information sharing threaten an agency's ability to influence the decisions of senior executive branch officials? It's basi-

---

162 *See* KENNETH LIEBERTHAL, THE U.S. INTELLIGENCE COMMUNITY AND FOREIGN POLICY: GETTING ANALYSIS RIGHT (2009) 9–12, *available at* http://www.brookings.edu/papers/2009/09_intelligence_community_lieberthal.aspx (click "Download Paper").

163 *See* ZEGART, *supra* note 38, at 68; *see also* Lieberthal, *supra* note 162, at 10–12 (noting that "President Bush assigned such importance to the PDB that, within the [intelligence community], getting an item into the PDB became a major goal of analysts").

164 *See* WMD REPORT, *supra* note 2, at 14, 181–82.

165 *See id.*

166 *Cf.* LIEBERTHAL, *supra* note 162, at 10–12.

167 *See* LOWENTHAL, *supra* note 78, at 187; POSNER, SURPRISE ATTACKS, *supra* note 1, at 115.

168 *See, e.g.*, WMD REPORT, *supra* note 2, at 189–92; POSNER, UNCERTAIN SHIELD, *supra* note 7, at 34.

169 *See* WMD REPORT, *supra* note 2, at 189–92.

cally a free-rider problem.[170] Intelligence agencies worry that, if a competitor uses shared data to enhance its analytical products, the credit for any intelligence breakthroughs will go to the recipient rather than the originator.[171] In other words, sharing produces benefits—better assessments, and therefore autonomy and influence—that originating agencies will not capture for themselves and that instead will accrue to their bureaucratic rivals. Free-riding concerns will be especially great when the recipient agency directly competes against the originator (e.g., both the FBI and NSA collect SIGINT, or signals intelligence[172]) than when the recipient is a more remote rival. The problem is exacerbated by the chronic uncertainties that plague the intelligence community about how to measure the value of information. It is prohibitively difficult, and maybe even impossible, for an agency that is considering a reciprocal sharing arrangement to assess how the data to be traded will improve either its own intelligence outputs or those of its rivals. Because of those valuation difficulties, the agency can't easily gauge how a data swap will affect the relative distribution of influence.

In other words, an agency will consider several values when deciding whether to enter a reciprocal sharing arrangement. Consider a hypothetical transaction involving two parties, the FBI and CIA. Value *A* is the value to CIA (i.e., to CIA's analytical outputs) of information in CIA's possession. Value *B* is the value to CIA of information in the FBI's possession. And value *C* is the value to the FBI of information in CIA's possession. Under what circumstances would a rational agency enter the arrangement? If this were a transaction involving two private firms, a rational party would go ahead with it if the firm's expected net profits from the exchange were greater than zero. It wouldn't matter to the firm whether the transaction also enriched its trading partner, or even if the transaction produced greater

---

170 *See* Amitai Aviram & Avishalom Tor, *Overcoming Impediments to Information Sharing*, 55 ALA. L. REV. 231, 235 (2004) (arguing that, in the private sector, "sharing information entails, besides the costs of collecting and disseminating information, the cost of losing a competitive edge over rivals that benefit from the information").

171 *See* RICHARD A. POSNER, COUNTERING TERRORISM: BLURRED FOCUS, HALTING STEPS 84 (2006) [hereinafter POSNER, COUNTERING TERRORISM]; POSNER, SURPRISE ATTACKS, *supra* note 1, at 113; Ronald D. Lee & Paul M. Schwartz, *Beyond the "War" on Terrorism: Towards the New Intelligence Network*, 103 MICH. L. REV. 1446, 1474 (2005) (book review). Aviram and Tor refer to this problem as "degradation"—i.e., "the private costs competitors must bear when sharing private information to their rivals' benefit." Aviram & Tor, *supra* note 170, at 234.

172 *See* Federal Bureau of Investigation, Directorate of Intelligence, http://www.fbi.gov/intelligence/di_ints.htm (last visited Sept. 30, 2009); National Security Agency, Signals Intelligence, http://www.nsa.gov/sigint/index.shtml (last visited Sept. 30, 2009).

profits for the partner than for it. All that matters is that the exchange enhances the firm's net welfare. The calculus for intelligence agencies is very different, because influence is a zero-sum game (or nearly so). Any enhancement of CIA's influence means a diminution of the FBI's influence; if the President is listening to the former more, he's listening to the latter less.[173] In other words, sharing is not a mutually beneficial trade. A rational agency thus will share, not if value *B* exceeds zero, but if value *B* exceeds value *C*—i.e., if CIA expects the arrangement to benefit it more than it expects the arrangement to benefit its rival the FBI.

The problem is that, although value *A* is largely known to CIA, values *B* and *C* are largely unknown. CIA knows how its own information will assist its analytical outputs. But the agency doesn't know what information the FBI has, and it therefore can't gauge how the data it stands to gain from the sharing arrangement will improve CIA's products (and hence its relative influence). Nor does CIA know how the information it has might assist the FBI, and it therefore can't estimate how the arrangement might improve the bureau's products (and hence its relative influence—or, to say the same thing, how the arrangement might diminish CIA's relative influence). This is a classic case of information asymmetry. CIA knows better than the FBI how CIA's data will benefit the intelligence enterprise, while the FBI knows better than CIA how the FBI's data will benefit the intelligence enterprise. Agencies' reluctance to enter sharing arrangements apparently stems from an institutional culture of risk aversion, which I discuss later.[174] They apparently calculate that, however great the magnitude of value *B*, there's a risk that value *C* is even greater. And agencies evidently aren't willing to take the gamble.

The second thing intelligence agencies maximize is autonomy—i.e., turf. An agency will want to pursue priorities that are important to its leadership or employees (or both) notwithstanding the priorities of other entities (such as a rival agency, superiors at the White House, or authorizers and overseers in Congress).[175] This is not to say agen-

---

173 *See* ZEGART, *supra* note 38, at 58, 68.

174 *See infra* Part III.D.

175 *See* WILSON, *supra* note 154, at 180–83 (arguing that "[a]gencies ranking high in autonomy have a monopoly jurisdiction (that is, they have few or no bureaucratic rivals and a minimum of political constraints imposed on them by superiors)"; they also have "identity or mission—a widely shared and approved understanding of the central tasks of the agency"); *see also* Levinson, *supra* note 8, at 933 (explaining that "bureaucrats may be committed to the missions of their agencies: protecting the environment, enforcing civil rights, educating children, and the like").

cies invariably engage in "empire-building."[176] Sometimes an agency's quest for autonomy leads it to claim new responsibilities, as when the Food and Drug Administration asserted power to regulate tobacco products as "drugs" or "devices" under the Food, Drug, and Cosmetic Act,[177] thereby furthering its core mission of promoting public health.[178] But sometimes autonomy maximization takes the form of disclaimers of power.[179] For instance, the Army Corps of Engineers for many years declined to extend environmental protections to wetlands, notwithstanding fairly clear signals that Congress wanted it to do so.[180] The reason for the Corps's forbearance was its desire to pursue its traditional priority of overseeing the nation's navigable waterways. It feared that wetlands regulation would divert scarce resources away from its core priorities, and also that its lack of expertise in environmental matters would undermine its reputation for efficiency.[181] Likewise, the FBI for years resisted congressional calls to assume responsibility for narcotics investigations.[182] The FBI preferred to focus on its traditional mission of solving kidnappings, and it feared the drug problem would prove intractable and undermine its reputation as a competent problem solver.[183]

In the national-security setting, an agency's desire to maximize its autonomy often takes the form of a desire to pursue investigations over which it believes it has jurisdiction without ceding control to rival agencies. Agency plays for autonomy are likely to be especially pronounced at the bureaucratic seams—areas where more than one agency plausibly might claim jurisdiction over a given investigation or subject matter.[184] One of the most pronounced fault lines is between the FBI and CIA, both of which have wanted to take the lead in do-

---

176 *See* Levinson, *supra* note 8, at 934–35; Todd J. Zywicki, *Institutional Review Boards as Academic Bureaucracies: An Economic and Experiential Analysis*, 101 NW. U. L. REV. 861, 873 (2007); *see also* James Q. Wilson, *The Politics of Regulation*, *in* THE POLITICS OF REGULATION 357, 376 (James Q. Wilson ed., 1980) ("Government agencies are more risk averse than imperialistic. They prefer security to rapid growth, autonomy to competition, stability to change.").

177 21 U.S.C. §§ 301–399 (2006).

178 *See* FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 125 (2000).

179 *See* Levinson, *supra* note 8, at 933, 935.

180 *See* Nathan Alexander Sales & Jonathan H. Adler, *The Rest Is Silence:* Chevron *Deference, Agency Jurisdiction, and Statutory Silences*, 2009 U. ILL. L. REV. 1497, 1504 (2009).

181 *See id.*

182 *See id.*

183 *See id.*; WILSON, *supra* note 154, at 182–95.

184 *See* Lerner, *supra* note 1, at 494 (arguing that hoarding is "the predictable result of having various bureaucracies with overlapping jurisdictions and competing claims to preeminence").

mestic counterespionage operations.[185] Imagine that an employee of the Nuclear Regulatory Commission is spying for Russia, feeding his control agents information about American nuclear-power capabilities. CIA will want to maintain control over the investigation and "turn" the mole into a double agent who can be used to feed the Russians misinformation (a basic counterespionage technique).[186] At the same time, CIA will want to prevent the FBI from investigating and ultimately prosecuting the spy—the attendant publicity would alert Russia that the mole's cover has been blown, eliminating his usefulness as a possible source of misinformation. The FBI will have different priorities. The bureau will want to prosecute the spy for violations of any number of federal laws criminalizing espionage (and maybe even treason), and it will not take kindly to CIA's efforts to insulate the mole from prosecution.[187]

There is some anecdotal evidence that agencies with national-security responsibilities seek to maximize their autonomy to conduct operations as they see fit and, concomitantly, to minimize the ability of competitors to do the same. Again, the traditional CIA-FBI rivalry is a rich source of examples. The night of October 21, 1942, operatives from the Office of Strategic Services ("OSS")—CIA's predecessor agency—mounted a black-bag job at the Spanish embassy in Washington, DC.[188] The spies were to retrieve and copy a cipher tape from an embassy safe, so as to better eavesdrop on Axis communications.[189] Somehow the FBI learned of the operation. J. Edgar Hoover dispatched a team of agents to the embassy with orders to arrest the OSS team.[190] They arrived in a squad car, with lights and sirens blaring—risking the CIA operatives' cover and bringing the operation to a noisy end.[191] "On the eve of landings in North Africa, . . . Hoover's men had come dangerously close to exposing key Allied cipher operations."[192]

How does information sharing threaten agency autonomy? In a word, it puts bureaucratic competitors on notice. Data exchange alerts agencies to the fact that their rivals' operations might implicate

---

185 *See generally* MARK RIEBLING, WEDGE: FROM PEARL HARBOR TO 9/11: HOW THE SECRET WAR BETWEEN THE FBI AND CIA HAS ENDANGERED NATIONAL SECURITY (2002).

186 *See* Banks, *supra* note 3, at 1151.

187 *See id.*; LOWENTHAL, *supra* note 78, at 157–58.

188 *See* RIEBLING, *supra* note 185, at 40–42.

189 *See id.*

190 *See id.*

191 *See id.*

192 *Id.* at 42.

their interests, giving them an opportunity to muscle in and take control.[193] If the FBI is leading the investigation of the Russian spy at the Nuclear Regulatory Commission, it will have an interest in keeping CIA in the dark. Alerting its rival that it has uncovered a mole working for Moscow will almost certainly cause CIA to demand a seat at the decisionmaking table, and to resist FBI's efforts to do what it does best—mount a criminal investigation with an eye toward ultimate (and very public) prosecution. CIA's seat at the table—and its efforts to promote its own interests—inevitably means the FBI will lose at least some control over the investigation. And if CIA is a savvy enough turf warrior, it might elbow the FBI out altogether. It should come as no surprise, then, that agencies—especially rival agencies that have overlapping areas of responsibility—resist information sharing as a way of preserving their ability to pursue autonomously their own priorities.

B. Information Sharing as an Intellectual-Property Problem

The reluctance of intelligence agencies to share information resembles problems that often arise in the IP context. IP law thus furnishes one theoretical lens through which to view the tendency of agencies to hoard. It's not quite right to suggest, as Judge Posner has said, that a given agency analyst "has no intellectual property right" in the intelligence information he generates.[194] It's true that individual employees might not have property interests in intelligence. But the agencies themselves have something very like an intellectual property right in the raw information they collect and the finished intelligence assessments they produce.

For starters, intelligence agencies enjoy something like a right to exclude others from their sensitive data, which is "one of the most essential sticks in the bundle of rights that are commonly characterized as property."[195] This right to exclude derives from classification standards and other information-access rules.[196] If a given piece of information is designated "Confidential," the agency may exclude persons (both within the agency and without) who lack at least a Confidential security clearance from gaining access to it. If the data is

---

193 *See* Lee & Schwartz, *supra* note 171, at 1474.

194 POSNER, SURPRISE ATTACKS, *supra* note 1, at 113. *But see* POSNER, UNCERTAIN SHIELD, *supra* note 7, at 17 (indicating that an intelligence agency "can assert a form of 'intellectual property' right over its data and analysis").

195 Kaiser Aetna v. United States, 444 U.S. 164, 176 (1979).

196 *See* LOWENTHAL, *supra* note 78, at 76, 153–54; POSNER, COUNTERING TERRORISM, *supra* note 171, at 85.

marked with the even more rarefied classification "Top Secret/Secure Compartmented Information," still more potential users are excluded. (For some compartments, the name of the classification level is itself classified.) A security clearance is a necessary but not sufficient condition of gaining access to information: an agency may exclude persons who hold the necessary clearances if they lack the requisite "'need to know'"[197]—i.e., those who don't require the data to do their jobs properly.[198]

Intelligence agencies also have the right to use the sensitive information they possess. They can synthesize it with other pieces of data to produce entirely new assessments, they can use it to determine where to deploy their scarce surveillance resources, and so on. Finally, agencies have something like a right to alienate national security information. We've already discussed how agencies can "sell" intelligence assessments to senior executive branch policymakers. They also can swap data with one another, or give it away to peers with no strings attached. For instance, the Department of Homeland Security might agree to provide the State Department with information about travelers who are processed at the nation's borders, in return for access to databases about foreigners who apply for visas at U.S. consulates overseas. These agencies effectively are operating in a barter economy (although the number of such exchanges is probably suboptimally low).

If intelligence agencies have a quasi-property interest in their national security data, then to what IP species does it belong? The most obvious candidate is trade secrets.[199] A trade secret is business infor-

---

197 POSNER, COUNTERING TERRORISM, *supra* note 171, at 85.

198 Intelligence agencies have not only a *right* to exclude others from sensitive information, but in some cases an affirmative duty to do so. The Espionage Act of 1917 and other federal laws impose criminal sanctions on those who disclose classified information to persons not authorized to receive it—for example, persons without the requisite security clearances. One statute makes it a crime for a federal official who holds information that he "has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation," to provide the data "to any person not entitled to receive it." 18 U.S.C. § 793(d) (2006). Another law makes it a crime to give "an unauthorized person" information about "the communication intelligence activities of the United States." *Id.* § 795(a)(3). The meaning and scope—and constitutionality—of the Espionage Act in particular are notoriously uncertain, *see generally* Harold Edgar & Benno C. Schmidt, Jr., *The Espionage Statutes and the Publication of Defense Information*, 73 COLUM. L. REV. 929 (1973), but the general thrust of these laws is fairly straightforward: agencies have an obligation, enforceable by criminal sanctions, to keep certain classified information out of unauthorized hands.

199 *See* POSNER, UNCERTAIN SHIELD, *supra* note 7, at 17 (suggesting that intelligence information is "akin to trade secrecy in the commercial sphere"). Three other possibilities can be dismissed out of hand. Intelligence information isn't a trademark, since it doesn't involve the

mation that derives value from the fact that it is not generally known, and that its owner strives to keep secret.[200] "By definition a trade secret has not been placed in the public domain."[201] If Kentucky Fried Chicken publicizes its secret blend of eleven herbs and spices, it no longer has a legally protected interest in that piece of intellectual property.[202] The Colonel now faces the prospect of his commercial rivals—Popeye's, Bojangles', and so on—free-riding on his recipe and improving their own chicken. Intelligence agencies prize secrecy as well: the value of an agency's sensitive data depends on its ability to shield that information from competitors. If the FBI discloses information to CIA, the information loses its value to the bureau, and indeed becomes a threat in the hand of its rival. CIA can free ride on FBI data, combining it with its own information and improving its analytical outputs. That increases the likelihood that intelligence consumers will buy more CIA products and fewer of the FBI's—i.e., the FBI's relative influence over policymakers might wane. Also, if the FBI divulges a trade secret, CIA might elbow its way onto what the bureau regards as its turf—i.e., the FBI's autonomy might be compromised. With trade secrets and intelligence alike, a piece of information is valuable to the owner only as long as it remains confidential. (The analogy is not perfect. When a private firm discloses a trade secret, the effect is that it surrenders a legally cognizable property interest. When an intelligence agency discloses information, it does not lose a property interest per se; it still retains the rights to use, exclude, and alienate. Instead, the value of the property interest the agency retains diminishes, perhaps to zero. The economic effect is the same, but the form the harm takes is different.)

---

use of a name, logo, or image to signal that it was produced by a particular agency. An agency's objective is not simply to brand intelligence information as somehow belonging to it, but rather to prevent rival agencies from acquiring it at all. Nor does national security data resemble patent or copyright. Those disciplines concern protections for business assets that have been publicly disclosed. *See, e.g.*, J.E.M. Ag Supply, Inc. v. Pioneer Hi-Bred Int'l, Inc., 534 U.S. 124, 142 (2001) ("The disclosure required by the Patent Act is 'the *quid pro quo* of the right to exclude.'"). By contrast, information-sharing problems involve agency assets—namely, raw intelligence and finished assessments—that have not been disclosed to others.

200 *See* UNIF. TRADE SECRETS ACT § 1(4), 14 U.L.A. 536, 538 (2005); *see also* RESTATEMENT OF TORTS § 757 cmt. b (1939).

201 Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 484 (1974).

202 *See* Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002 (1984) ("Information that is public knowledge or that is generally known in an industry cannot be a trade secret. If an individual discloses his trade secret to others who are under no obligation to protect the confidentiality of the information, or otherwise publicly discloses the secret, his property right is extinguished." (citation omitted)).

Intelligence resembles trade secrets in another important way. Both systems contemplate that an owner may share with others in a way that does not strip the information of all value. A private firm may agree to provide another company with access to its trade secret; the originating firm retains a legally cognizable interest in the secret so long as the recipient is duty bound not to share the data with others.[203] Sometimes the confidentiality obligations are explicit contractual terms; sometimes courts imply them.[204] The key point is that the presence of restrictions on the further distribution means the originating firm still enjoys an interest in the trade secret. A similar mechanism exists in the intelligence context. One agency might agree to let another have access to a piece of sensitive information subject to ORCON restrictions that bar the recipient from further sharing the data.[205] For instance, an interagency memorandum of understanding might call for DHS to share its threat assessments of U.S.-bound foreigners with the State Department, in return for the latter's pledge not to further distribute the assessments. This sort of transaction preserves the assessments' value to DHS—the restriction keeps other competitors in the dark—despite the fact that at least one rival now has access to them. ORCON restrictions, like confidentiality obligations, enable agencies to share information with a select recipient without facing the danger that widespread and uncontrolled dissemination will destroy the value of its trade secret.

In short, intelligence agencies shield their trade secrets from competitors just as private firms do. We are now in a better position to understand some of the information-sharing failures recounted above. Take, for instance, the wall.[206] FBI intelligence officials kept information behind the wall in part because hoarding promoted their influence. The wall prevented rivals—namely, criminal investigators at Main Justice—from free riding on intelligence officials' products, and using that data to enhance the advice they provided to senior decisionmakers. Information was valuable to the spies precisely because it was kept secret. If the cops had access, the data would have been worthless (or nearly so). The rational course for an influence-seeking agency therefore was to keep the information secret the same way a

---

203 *See* UNIF. TRADE SECRETS ACT § 1(2), 14 U.L.A. at 537 (defining "misappropriation" to include "use of a trade secret" by a person whose "knowledge of the trade secret was . . . derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use"); *see also* RESTATEMENT OF TORTS § 757 cmt. b.

204 *See, e.g.*, Smith v. Snap-On Tools Corp., 833 F.2d 578, 580 (5th Cir. 1987).

205 *See* LOWENTHAL, *supra* note 78, at 154.

206 *See supra* Part I.A.1.

profit-seeking restaurant keeps its recipe secret. The wall also promoted intelligence officials' autonomy: if the cops were out of the loop, they couldn't undermine the spies' control over operations. Criminal investigators might have urged that the targets be prosecuted immediately instead of remaining under surveillance. Or, even more dramatically, coordination between cops and spies might have led the FISA court to reject a surveillance application on the ground that its primary purpose was something other than foreign intelligence. To be sure, the FBI's intelligence officials and criminal investigators do not compete as directly as, say, two intelligence agencies or two law-enforcement agencies would. The two produce different outputs—cops generate prosecutions, spies generate efforts to turn, surveil, and interrogate. Yet the two are still rivals insofar as they compete for the same scarce DOJ budgetary resources, and insofar as an intelligence operation and a prosecution are rough substitutes for one another—i.e., two alternative means that senior officials could use to counter a particular threat.

Trade secrets also help explain the Department of Homeland Security's apparent success in persuading the President to exempt its special classes of data (such as critical-infrastructure data) from the new regime for controlled unclassified information.[207] DHS's quest for sharing exemptions may have been a play to preserve its influence in matters involving critical infrastructure—i.e., to prevent rivals from free riding on its outputs. If only DHS has access to information about vulnerabilities at chemical plants and nuclear facilities, then only DHS will be in a position to sell threat assessments to the President. DHS's successful bid to retain exclusive possession of critical-infrastructure information thus resembles a classic intellectual property problem. The agency had raw data—information about critical-infrastructure vulnerabilities—that could be used to prepare finished intelligence assessments, and it didn't want to share with rivals. The inputs were valuable to DHS precisely to the extent it was able to keep them out of competitors' hands. If the data had found their way to rival agencies, their value to DHS would have diminished, perhaps to zero.

207 *See supra* notes 92–96 and accompanying text.

C. . . . as an Antitrust Problem

Antitrust law offers a second lens to examine intelligence agencies' reluctance to share information.[208] The market for intelligence products is not one that many would describe as structurally competitive. The buyer's side consists of a single consumer—the presidency, including other senior policymakers who are appointed by or otherwise are accountable to the President. Intelligence agencies generally don't sell their products to consumers in the private sector, foreign governments, or even Congress. Senior executive branch policymakers are the only buyers. The intelligence market thus is something like a monopsony—a condition in which a single consumer exists for a particular good or service.[209] Sellers are nearly as concentrated. The overall market for intelligence products resembles an oligopoly—a condition in which only a handful of sellers exist to supply a particular good or service.[210] The intelligence oligopoly is insulated against competition by massive entry barriers.[211] No other administrative agencies—or private firms, for that matter—can enter the intelligence market unless Congress authorizes them to do so and appropriates the necessary funds; also, the executive branch would need to grant new entrants the requisite security clearances. If entry is difficult, exit is even harder. Agencies in the intelligence oligopoly have statutory duties to collect and analyze information. Unlike private firms, they cannot simply go bankrupt or otherwise leave the market unless Congress authorizes them to do so.

While the larger intelligence market resembles an oligopoly, there are smaller submarkets in which various agencies are domi-

---

208 Antitrust law frequently grapples with information-sharing problems. *See generally* Aviram & Tor, *supra* note 170. The issue typically arises when private firms want to exchange information with one another—e.g., information about industry best practices or compatibility standards. *See* David J. Teece, *Information Sharing, Innovation, and Antitrust*, 62 ANTITRUST L.J. 465, 473–78 (1994). The legal question is whether such sharing should be regarded as per se illegal, or whether its legality should be assessed under the rule of reason. The intelligence world presents the opposite problem. The problem here is not whether the sharing that is taking place is desirable (or lawful) or not. The problem is that sharing simply isn't taking place. The questions that interest me are whether antitrust law can help explain why intelligence agencies are reluctant to share, and whether antitrust-like solutions can encourage more sharing. See *infra* Part III.B.

209 *See* HERBERT HOVENKAMP, FEDERAL ANTITRUST POLICY: THE LAW OF COMPETITION AND ITS PRACTICE § 1.6b, at 14 (1994). *See generally* ROGER D. BLAIR & JEFFREY L. HARRISON, MONOPSONY: ANTITRUST LAW AND ECONOMICS (1993).

210 *See* HOVENKAMP, *supra* note 209, § 1.5c, at 37.

211 *See id.* § 12.4b5, at 473 ("[G]overnment regulation, licensing and entry restrictions collectively create among the greatest and most effective entry barriers.").

nant—such as the submarkets for analytical products based on SIGINT (signals intelligence) or GEOINT (geospatial intelligence, including satellite imagery). One of the reasons for agencies' niche dominance is that they have exclusive (or nearly exclusive) control over the different types of inputs used to produce finished assessments. Agencies exhibit a degree of vertical integration: they control assets at each stage of the intelligence-production cycle, from collection to analysis to distribution.[212] For example, the NSA's worldwide network of electronic eavesdropping equipment gives it a unique ability to collect phone calls and e-mails overseas,[213] which in turn yields a dominant NSA position in the submarket for SIGINT-based intelligence assessments. Similarly, the National Geospatial-Intelligence Agency's ("NGA") fleet of satellites gives it a unique ability to collect overhead imagery,[214] which translates to a dominant NGA position in the submarket for GEOINT-based assessments. Unlike a classic oligopoly, in which products are essentially undifferentiated, intelligence products are heterogeneous, at least in some circumstances. An NSA assessment will have different emphases than one prepared by the NGA. Both electronic surveillance and satellite imagery can shed light on the intentions and capabilities of an adversary, but they are not always perfect substitutes for one another.

These market conditions—monopsony, oligopoly, significant entry and exit barriers, dominance in submarkets, and heterogeneous products—seem likely to produce anticompetitive conduct among intelligence agencies. And market distortions have in fact emerged, especially as regards the sharing of information. For instance, one might think of agencies' refusal to share information as akin to a private firm unilaterally refusing to deal with a competitor. In the private sector, firms sometimes refuse to sell goods or services to rivals as a way of consolidating power in the relevant market.[215] Microsoft threatened to cancel the Apple version of its popular Office software to strengthen its hand in the market for Internet browsers.[216] Intelli-

212 *See id.* § 9.1, at 330.

213 *See generally* National Security Agency, Signals Intelligence, http://www.nsa.gov/sigint/index.shtml (last visited Sept. 29, 2009).

214 *See generally* National Geospatial-Intelligence Agency, GEOINT, https://www1.nga.mil/About/WhatWeDo/GeoInt/Pages/default.aspx (last visited Sept. 22, 2009).

215 *See* HOVENKAMP, *supra* note 209; *see also* United States v. Colgate & Co., 250 U.S. 300, 307 (1919) (observing that a private firm ordinarily may "exercise [its] own independent discretion as to parties with whom [it] will deal," but such refusals may be unlawful when the firm seeks "to create or maintain a monopoly").

216 United States v. Microsoft Corp., 253 F.3d 34, 72–74 (D.C. Cir. 2001).

gence agencies hoard for similar reasons. Just as private firms see unilateral refusals to deal as a way to enhance their market power (and ultimately to maximize their profits), intelligence agencies see unilateral refusals to share as a strategy for preserving power in their respective submarkets (and ultimately maximizing their influence and autonomy).

Consider CIA's decision to keep the FBI and State Department in the dark about an al Qaeda member (and eventual 9/11 hijacker) who had entered the United States.[217] The agency may have refused to deal because it feared that doing so would undermine its autonomy. Maybe the FBI would demand to take the lead in the investigation, replacing CIA at the helm.[218] Maybe the publicity associated with any eventual prosecutions would sour CIA's relationships with the Saudi intelligence officials who provided it with information about Nawaf al Hazmi and Khaled al Mihdhar. Maybe the FBI's involvement would complicate any efforts to turn the two men into CIA double agents. Likewise, the NSA initially may have refused to provide the FBI with transcripts of intercepted international phone calls to maintain its dominant position in the submarket for intelligence assessments based on overseas SIGINT.[219] Sharing would have enabled the FBI to compete against it in that submarket. As in the private sector, intelligence agencies refuse to deal to maintain power in their respective submarkets, and to prevent competitors from gaining footholds in niches they regard as their own.

Sometimes intelligence agencies seek to maintain and expand market power through rent seeking. In particular, agencies lobby policymakers to award them something akin to state-granted monopoly rights. One example is President George W. Bush's 2008 order establishing new rules to encourage the sharing of controlled unclassified information, or CUI.[220] The new CUI rules expressly exempt certain classes of data maintained by the Department of Homeland Security, such as information about vulnerabilities at chemical plants and other types of critical infrastructure.[221] The effect of the exemption is to establish a DHS monopoly in the submarket for critical-infrastructure intelligence, thus boosting DHS's influence. The CUI

---

217 *See supra* Part II.A.2.

218 *See* WRIGHT, *supra* note 44, at 352–54 (discussing CIA hostility toward lead FBI counterterrorism investigator).

219 *See supra* notes 98–102 and accompanying text.

220 *See supra* notes 82–96 and accompanying text.

221 *See supra* notes 92–96 and accompanying text.

exemption amounts to an exclusive deal.[222] Because DHS need not share critical-infrastructure data with its rivals, other agencies will be hampered in preparing vulnerability assessments. That in turn means that policymakers can only buy DHS product. DHS's monopoly rights also promote autonomy. The agency generally acquires critical-infrastructure information through voluntary submissions by private companies,[223] and firms understandably worry that proprietary business information might find its way into the hands of competitors. DHS may have feared that, if it could not promise confidentiality, firms would no longer turn over the information. And that would undermine its ability to achieve its regulatory priorities—counterterrorism, obviously, but also preparing plans to prevent and recover from infrastructure damage due to natural disasters like wildfires or hurricanes. The CUI monopoly ensures that DHS will continue to receive the information it deems necessary to achieving these regulatory objectives.

A third type of distortion in the intelligence market is the formation of cartels. In the private sector, oligopolists will want to fix prices or reduce output to levels that enable them collectively to recoup monopoly profits.[224] The problem is that it's difficult for firms to anticipate each others' pricing and output decisions. One solution is to form cartels, either through explicit agreements or tacit ones.[225] Price fixing isn't possible in the intelligence market, because the compensation agencies receive for their products is set by the President (and Congress). Agencies don't determine how much of the federal budget they will receive in exchange for a particular intelligence report, nor do they determine how much prestige, influence, and autonomy the assessment will yield them. In other words, agencies' oligopoly powers are offset by the monopsony power of the sole intelligence consumer—the Presidency. The upward price pressure the oligopoly otherwise would generate is offset by the downward price pressure of the monopsony. Because intelligence agencies can't fix prices, the cartels they form need to boost member profits—i.e., influence over senior policymakers and autonomy to pursue agency priorities—in more indirect ways. For instance, they might form a market-division

222 *Cf.* HOVENKAMP, *supra* note 209, § 10.8e, at 390 (discussing the legality of exclusive dealing in the context of private firms).

223 *See supra* note 97 and accompanying text.

224 *See* HOVENKAMP, *supra* note 209, § 4.1, at 140–41.

225 *See id.*; *cf.* United States v. Socony-Vacuum Oil Co., 310 U.S. 150, 218 (1940) (holding that price-fixing agreements are per se illegal under the Sherman Act).

cartel.[226] Such an arrangement would give each agency (or allow an agency to maintain) a formal position of dominance in a particular intelligence submarket—for instance, the FBI might be handed the domestic SIGINT niche, while the submarket for overseas SIGINT might be given to the NSA. The agencies then would agree not to compete against one another in their respective submarkets.[227] Information-sharing restrictions are an important way for agencies to maintain the boundaries of their respective niches.

This seems to be what happened in the Guideline 4 report.[228] Its stated objective is to facilitate the sharing of information obtained from foreign governments.[229] Yet it contains an exception that devours the rule: it accepts foreign ORCON restrictions.[230] Thus when the FBI enters an agreement with the United Kingdom's MI5 to exchange information about terrorist threats, the bureau may (in some unspecified sets of circumstances) agree to an MI5 request (or independently propose?) that the FBI not share any of the information it receives with other U.S. intelligence agencies. The effect is to preserve cartel members' respective influence over senior policymakers. By refusing to share information that relates to the submarkets in which they are dominant, agencies eliminate the possibility of facing new and unwelcome competition in the production of niche intelligence assessments. The FBI doesn't have to worry that DHS will use shared MI5 information to prepare analyses that compete with the FBI's own offerings. Cartel members thus mutually agree that they will continue to be the sole suppliers of particular types of intelligence products. The market-division arrangement also promotes cartel members' autonomy. As the Guideline 4 report recognizes, "it is not only the foreign partners but also the United States that will want to

---

226 *See* HOVENKAMP, *supra* note 209, § 5.2b4, at 190–92; *cf.* United States v. Topco Assocs., Inc., 405 U.S. 596, 607–08 (1972) (holding that geographic market division arrangements are per se illegal under the Sherman Act). Market division may be thought of as a more complete version of price fixing. A classic price-fixing arrangement involves firms agreeing not to compete against one another on price terms, though nonprice competition may occur. A market division amounts to an agreement among firms not to compete on any terms, at least within the relevant market.

227 *See* POSNER, SURPRISE ATTACKS, *supra* note 1, at 143–44 ("But often turf warriors decide they're better off colluding than competing, presenting the higher authorities not with a choice but with the bureaucratic equivalent of a division of markets."); JAMES Q. WILSON, THE INVESTIGATORS: MANAGING FBI AND NARCOTICS AGENTS 170 (1978) (arguing that bureaucrats know "instinctively what every natural executive knows: having a monopoly position on even a small piece of turf is better than having a competitive position on a large one").

228 *See supra* notes 74–81 and accompanying text.

229 *See* GUIDELINE 4 REPORT, *supra* note 77, at 1.

230 *See id.* at 11–12.

include such restrictions in information sharing agreements."[231] In other words, American intelligence agencies want to control how a foreign counterpart uses information they provide to it, and therefore they agree to reciprocal restrictions on data they receive from a foreign source. Hoarding also furthers agency autonomy by strengthening its relationships with overseas counterparts;[232] further dissemination might anger the foreign governments that provided the data, causing them to be less cooperative in the future.

One final observation about intelligence cartels. Private-sector cartels are notoriously difficult to form and maintain, not just because firms fear the resulting exposure to legal liability under the Sherman Act, but because of the potential gains from cheating.[233] Cartel maintenance seems easier in the intelligence context. Private cartels can face intense competition from outsiders that are tempted by oligopolistic prices to enter the market. Yet the barriers to entering the intelligence market are so severe that cartel members face little competition from new entrants, if any at all. Intelligence agencies also have fewer opportunities to cheat. Private firms will want to undercut their fellow cartel members by increasing their output or selling at a lower price. But intelligence agencies can't undercut, since they must take whatever price (budgets, prestige) the monopsonistic President gives them. Finally, while it can be difficult for private cartels to detect cheaters' output adjustments, the telltale signs that an intelligence agency is cheating—raiding another's turf—are easier to detect. Agencies naturally will monitor their rivals to make sure they're not muscling into areas they shouldn't be (as when, for example, the NSA detected the FBI's plan to build its own antennae for intercepting al Qaeda satellite phone calls,[234] and when the FBI detected the planned black-bag job at the Spanish embassy[235]).

D. . . . as an Organizational-Theory Problem

Organizational theory offers a third lens through which intelligence agencies' tendency to hoard might be understood.[236] Informa-

---

231 *Id.* at 9.

232 *See* LOWENTHAL, *supra* note 78, at 99 (noting that intelligence agencies strive to maintain foreign liaison relationships).

233 *See* George J. Stigler, *A Theory of Oligopoly*, 72 J. POL. ECON. 44, 46 (1964); *see also* HOVENKAMP, *supra* note 209, § 4.1, at 143–45.

234 *See supra* notes 98–102 and accompanying text.

235 *See supra* notes 188–92 and accompanying text.

236 *Cf.* Bibas, *supra* note 149, at 996–1016 (using organizational-theory principles to assess priorities in prosecutors' offices); Gregory S. McNeal, *Organizational Theory and Counterterror-*

tion sharing can be risky, and intelligence officials are conditioned by their agencies' respective institutional cultures to avoid risks.[237] Sharing might expose them to blame for any resulting diminution in their agencies' respective levels of influence and autonomy. Even worse, sharing could violate the law, and officials could face personal criminal liability. This is why FBI intelligence officials were told in the 1990s that sharing information was a "career stopper."[238] The result is a fairly predictable chilling effect: intelligence officials contemplating a sharing arrangement will halt well short of where they think the legal cliff might be to avoid falling into the abyss.[239] The intelligence system lacks the structures needed to manage these risks. In its current configuration, the system is essentially powerless to mitigate officials' cultural tendencies to hoard and to incentivize them to share in ways that are desirable yet risky.

Certain schools of organizational theory explain the behavior of private firms and other collective entities as the result of their respective institutional cultures. "Culture is to the organization what personality is to the individual—a hidden, yet unifying theme that provides meaning, direction, and mobilization."[240] On this account, an organization's actions are determined as much by its employees' unspoken assumptions, values, norms, and interests as by the entity's structure, policies, and leadership. "[T]he harder-to-see aspects of organizational life—such as training, procedures, cultures, and agency strictures—often matter more."[241] In a nutshell, organization behavior is the sum of individual employee behavior, and individual em-

---

ism Prosecutions: A Preliminary Inquiry, 21 REGENT U. L. REV. 306, 325–329 (2009) (using organizational-theory principles to assess the Justice Department's creation of the new National Security Division).

237 *See* Banks, *supra* note 3, at 1152–53, 1172; Lerner, *supra* note 1, at 505.

238 *See* Kris, *supra* note 1, at 501; *see also* 9/11 COMMISSION REPORT, *supra* note 2, at 79.

239 This is not to deny that this chilling effect may have some salutary consequences. If agency officials are reluctant to push the envelope, that means they are less likely to undertake questionable and sometimes clearly unlawful surveillance, such as the FBI's wiretapping of Martin Luther King, *see* POSNER, UNCERTAIN SHIELD, *supra* note 7, at 133, or CIA's surveillance of domestic antiwar activists, *see* INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS: FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, bk. 2, S. REP. NO. 755, at 96 (1976) [hereinafter CHURCH COMMITTEE REPORT].

240 RALPH H. KILMANN, MARY J. SAXTON & ROY SERPA, GAINING CONTROL OF THE CORPORATE CULTURE ix (1985).

241 ZEGART, *supra* note 38, at 10; *see also* Bibas, *supra* note 149, at 999 (indicating that employees "are shaped by hiring, firing, pay, and promotion policies," as well as "by an organization's structure, procedures, physical layout, folklore, and mission statement" (citing EDGAR H. SCHEIN, ORGANIZATIONAL CULTURE AND LEADERSHIP 233–42 (1985))).

ployee behavior is the product (at least in part) of the surrounding institutional culture.

The intelligence community's institutional culture appears to be one of risk aversion.[242] That cultural trait is not an accident; it is the product of specific incentive structures within intelligence agencies. Officials tend to be risk averse because the schedule of career rewards and penalties creates powerful incentives to avoid bold and independent action. An official's career typically will be hurt more if he takes a bold action that turns out to be harmful than it will be advanced if he takes a bold action that turns out to be beneficial.[243] The expected costs of boldness exceed the expected benefits, and that asymmetry naturally inclines the official to avoid risks.[244] Notice that I am not using the expression "risk averse" in its technical sense. I do not mean to suggest that, when facing positive and negative outcomes of equal expected magnitude, intelligence officials systematically will weigh the negative ones more heavily. My claim is that they often face negative outcomes that are in fact greater than the positive outcomes.

Consider a simple decision that officials throughout the government's national security apparatus must make each day. An analyst is asked to advise his superiors whether a foreign power represents a threat to the United States. He can make either of two assessments: he can go along with the consensus opinion shared by his peers or he can offer a bold and unorthodox opinion shared by no one else. Assume further that the analyst's assessment can be either right or wrong, and that his superiors can precisely measure the quality of his report. (Those assumptions may not be realistic. Intelligence assessments can be partially correct or erroneous in a way this simple binomial hypothetical doesn't account for, and "the contribution of the individual intelligence officer to [an agency's] output elude[s] measurement."[245]) Which option would a rational analyst pick?

---

242 Some scholars believe that government employees as a group are systematically more risk averse than their private-sector counterparts. Evidence is found in the willingness of government employees to forego the chance of higher salaries in the private sector in exchange for greater protections against performance-related firings. *See, e.g.*, Don Bellante & Albert N. Link, *Are Public Sector Workers More Risk Averse than Private Sector Workers?*, 34 INDUS. & LAB. REL. REV. 408, 408–12 (1981).

243 *See* POSNER, UNCERTAIN SHIELD, *supra* note 7, at 42–43.

244 *Cf.* JACK GOLDSMITH, THE TERROR PRESIDENCY 90–98 (2007) (discussing reasons for intelligence agencies' risk aversion); POSNER, UNCERTAIN SHIELD, *supra* note 7, at 42–44 (same).

245 POSNER, UNCERTAIN SHIELD, *supra* note 7, at 62.

To answer that question, we need to know about the credit the analyst will receive if his assessment proves correct, and the blame he'll incur if he's wrong. If the analyst goes along with a consensus that proves erroneous, the blame will be diffused among everyone who shared it. The analyst will not be singled out for any special sanctions, and if the herd is large enough it's doubtful that anyone will be punished; you can't simply fire, demote, or reassign an entire division of an agency.[246] In other words, the per capita cost to an analyst of propounding a consensus (and ultimately erroneous) opinion is quite low. The same would be true if the analyst subscribes to a consensus view and the herd turns out to be right: credit for the accurate assessment will be distributed among a large group; the per capita benefit of propounding a consensus (and ultimately accurate) opinion is quite low. Now consider the rewards and punishments an analyst would face if he struck out on his own and offered a bold, unorthodox assessment. Suppose he gets it wrong. Now there's a scapegoat. Blame for the erroneous assessment can be laid squarely at the feet of the one person who made it. In other words, the per capita cost to an analyst of propounding an unorthodox (and ultimately erroneous) opinion is considerable. Suppose the analyst's bold assessment turns out to be accurate. Now there's a hero. The prescient analyst can be singled out for special rewards; the per capita benefit of propounding an unorthodox (and ultimately accurate) opinion is considerable.[247] These possibilities can be illustrated in a basic matrix:

	Correct	Incorrect
Consensus	(1) Credit diffused; low per capita benefit	(2) Blame diffused; low per capita cost
Unorthodox	(3) Full credit; high per capita benefit	(4) Full blame; high per capita cost

Why isn't it a wash? Why aren't the high costs of a bold (but erroneous) assessment (value 4) offset by the high benefits of a bold (and prescient) assessment (value 3), leaving a rational employee agnostic as between the two? The reason is that, at least for intelligence agencies (and maybe for other government agencies as well), value 3

246 For instance, to my knowledge, none of the CIA analysts who shared the consensus (and ultimately erroneous) view that Saddam Hussein's Iraq had and was seeking weapons of mass destruction was disciplined.

247 But not always. The FBI analyst who correctly predicted that al Qaeda member Khaled al Mihdhar might participate in a terrorist attack, *see supra* notes 67–73 and accompanying text, does not appear to have been rewarded for his prescience.

always (or nearly always) will be systematically smaller than value 4. An analyst usually stands to lose more from offering an unorthodox assessment that ends up being wrong than he stands to gain from offering an unorthodox assessment that turns out to be right.[248] This is so because government employers have relatively few carrots with which to reward employee excellence. Unlike private industry, public-sector managers have very little ability to reward high-performing employees with sizeable raises. The government payscale usually moves in lockstep, raises are more due to seniority than performance, and salaries top off at relatively modest levels (compared to the private sector). Nor are government managers able to give superstar employees performance bonuses akin to what their private-sector counterparts offer. To be sure, high-performing agency employees can derive some non-monetary income from a job well done—e.g., psychic rewards, professional prestige, and enhanced reputation among their peers. But it seems just as probable that a superstar analyst will provoke resentment and jealousy among the herd, whose members will wish that they had taken a chance by making a bold assessment.

Now consider the sticks. A government manager may not have the same power to discipline underperforming employees as in the private sector, but he has enough sticks to leave a mark. An analyst whose intelligence assessments repeatedly turn out to be mistaken could be punished in any number of ways. He could be reassigned to a job that involves less prestigious work or a less desirable venue—the American equivalent of guarding *zeks* in Siberia.[249] In more extreme cases he could be demoted, losing both prestige and income. In the most extreme cases the analyst could lose his job, either because the agency formally terminates him (rare), or because he has suffered a massive loss of prestige and is informally forced out (more common). A rational intelligence officer, aware of these possibilities, will tend to follow the herd. Why put your neck on the line and risk transfer, demotion, termination, and worse, when there is very little to gain from doing so? The safer course is to avoid boldness altogether.[250]

---

248 POSNER, UNCERTAIN SHIELD, *supra* note 7, at 42–43.

249 *Cf.* ALEKSANDR SOLZHENITSYN, ONE DAY IN THE LIFE OF IVAN DENISOVICH (Victor Gollancz Ltd. trans., Penguin Books 2000).

250 Different types of intelligence officials may have different tolerances for risk. Analysts seem to be particularly risk averse, for the reasons given above. But the incentive structure may well be different for others, such as operatives in CIA's National Clandestine Service (formerly the Directorate of Operations), which conducts covert operations like paramilitary activities. These officials likely derive significant psychic income from their jobs—e.g., feelings of exhilara-

How, then, is information sharing risky? The asymmetries between rewards and penalties are especially pronounced in the context of data exchange. An employee who decides to share his agency's product with a bureaucratic rival stands to gain very little if the exchange pays off and the competitor agency achieves an intelligence breakthrough. Maybe the analyst gets an attaboy from the grateful recipient, but his salary won't go up and he's not going to win a promotion. To the contrary, the analyst has a lot to lose. Sharing may cause the originating agency to suffer a relative loss of influence and autonomy, and the employee who handed data to the rival is likely to be blamed. The expected costs are great indeed. And those are just the costs of a *successful* exchange of data—i.e., sharing that produces an intelligence breakthrough. What about the costs of an *unsuccessful* exchange? An analyst who shares information can expect to be personally blamed if the competitor leaks the data to a newspaper, if a foreign intelligence service acquires the information by penetrating the competitor, if the agency's sensitive sources and methods are compromised as a result of the sharing, and so on.

The costs of information sharing can be even greater than blame for the loss of influence and autonomy. Data exchange also threatens to expose agency employees to personal criminal liability. The problem results from uncertainty. The laws that govern government access to and use of information are not always drafted with the precision of Justinian. Even after the USA PATRIOT Act, a great deal of uncertainty remains about whether various kinds of data may be shared. That haze of legal ambiguity makes it difficult—and sometimes impossible—for agency officials to know what the limits are.[251] Some are even buying insurance to cover their legal expenses in the event they face criminal charges.[252] Given this uncertainty, a rational agency official may choose not to share for fear of exposing himself to legal liability. As in the private sector, legal ambiguity produces inefficiencies. Because of liability concerns, intelligence agencies fail

---

tion from participating in a successful strike on an al Qaeda training camp—and the psychic income may be greater the riskier the endeavor. In other words, the benefits of bold action may be greater for covert operatives than for other intelligence professionals. If the expected benefits of boldness (including psychic income) are equal to (or greater than) the expected costs, these officials will be risk neutral (or risk seeking).

251 *Cf.* BENJAMIN WITTES, LAW AND THE LONG WAR 188 (2008) (noting, in reference to interrogation, that "[w]e are, in short, asking men and women in the service of their country to live their professional lives standing on and leaning over the border of criminal conduct we lack the courage to define precisely").

252 *See* GOLDSMITH, *supra* note 244, at 95–96.

to participate in information exchanges that would yield a net increase in social welfare. The result is a deadweight loss—lower quality intelligence assessments, less informed policy decisions, and so on.

A number of federal statutes might result in criminal liability for officers who share various types of information. For example, the Trade Secrets Act makes it a crime for agency employees to disseminate proprietary business information except where "authorized by law."[253] An official who flouts the act faces a year in jail, a criminal fine, and loss of government employment.[254] The problem is that the category of persons "authorized by law" to see the data is hardly a crisply defined set. As such, a DHS official who has received proprietary information from, say, a private chemical plant, will think twice before sharing with others who might help protect the plant's vulnerabilities or respond to an attack, such as state and local police. Similarly, the Posse Comitatus Act makes it a crime for the armed forces to participate in domestic law enforcement, punishable by two years imprisonment and criminal fines.[255] That restriction may impede information sharing and other coordination between civilian and military authorities. For instance, DHS might be reluctant in the run-up to the annual hurricane season to share its disaster-response plans with the Pentagon or with National Guard units in coastal states. (In addition to laws backed by criminal sanctions, other statutes might restrict sharing. For instance, the National Security Act of 1947 bars CIA from engaging in any "internal security functions,"[256] which might impede sharing and coordination with the FBI and other domestic law-enforcement entities. The Privacy Act of 1974 bars agencies from sharing information except pursuant to a "routine use" that has been published in the Federal Register.[257]) In these and other cases, the rational thing for an official to do—assuming that he wants to stay out of jail—is to stop well short of sharing that approaches the hazy legal limits.

Not just individual officers, but agencies themselves would suffer fallout if courts determined that a decision to share information crossed a legal line. An agency that violates the law will take a significant—perhaps catastrophic—hit to its reputation, and those reputation costs will threaten its influence and autonomy. The more

253 *See* 18 U.S.C. § 1905 (2006).

254 *See id.*

255 *See id.* § 1385.

256 50 U.S.C. § 403-4a(d)(1) (2006).

257 5 U.S.C. § 552a(b)(3) (2006).

violations, the greater the costs will be. For reasons of political self-interest, the President and other policymakers will want to keep at arm's length agencies that have become controversial due to their illegal activities. The inevitable result is that the controversial agency will see its influence dwindle, and perhaps waste away altogether; no policymaker will want to be seen as taking the advice of a scofflaw.[258] The same calamitous harms may befall the agency's autonomy. Over the short run, an agency whose sharing has been held unlawful will find it harder to achieve the priorities the data exchange was meant to support. If a court held it was a violation of the Posse Comitatus Act for DHS to share disaster-response plans with the military, a core DHS function—preparing for, responding to, and recovering from natural disasters—would be imperiled. The long run consequences would be even more dire. Intelligence agencies that have become controversial will find their rivals carving away pieces of their turf. An agency's ability to hold its turf ultimately depends on its access to its superiors, and that won't be possible if policymakers are shunning it.

Note that a conviction isn't necessary for these reputational harms to materialize. Mere allegations that an agency unlawfully shared information can be enough to diminish its influence and autonomy. Consider CIA's weakened position after the release of the Church Committee reports in the mid-1970s. The reports accused the agency of systematic legal violations over many years, including wiretapping domestic dissident groups, opening mail, participating in assassinations, interfering in foreign elections, and so on.[259] Even without formal criminal charges, let alone convictions, the allegations by themselves were enough to hobble CIA for a generation. The agency suffered a catastrophic loss of reputation that led to smaller budgets, stricter legal limits on its ability to operate, and a loss of influence.[260] The point is not that these outcomes were or were not justified responses to the Church Committee's findings. What's relevant is that significant reputational harms can accrue even from mere accusation. Agencies are well aware of that fact and they act accordingly.[261]

---

258 The President will have an interest in not appearing to rely on the controversial agency. But he might continue to consult the agency if he is able to do so in secret, which would leave the agency's influence intact. Still, the President, who is accustomed to living in a fishbowl, may conclude that his private reliance on the controversial agency is likely to become public knowledge, and for that reason he may decline to do so even behind closed doors.

259 *See generally* CHURCH COMMITTEE REPORT, *supra* note 239.

260 *See* COLL, *supra* note 44, at 43–44.

261 These incentives may be reversed in times of crisis. Professor Jack Goldsmith—onetime

The wall is an example of cultural risk aversion that resulted in hoarding.[262] The Justice Department didn't build the wall between cops and spies because it was thought to be legally necessary.[263] To the contrary, the agency was quite clear that its sharing restrictions "go beyond what is legally required."[264] What DOJ feared was legal uncertainty: How would the FISA court apply the primary-purpose standard?[265] It also worried that appearance problems—namely, indications that criminal investigators were directing FISA surveillance in an end run around the more rigorous Title III standards—would lead the FISA court to reject surveillance applications, thereby interfering with the agency's core mission of detecting and interdicting terrorist threats.[266] So the agency, out of an abundance of caution, adopted a prophylactic rule that disfavored sharing. No wonder intelligence officials—and therefore the agencies they serve—are reluctant to share information. They have little to gain from doing so and much to lose.[267]

---

head of the Justice Department's Office of Legal Counsel—has described the "cycles of timidity and aggression" to which officials in America's national security apparatus are subject. GOLDSMITH, *supra* note 244, at 163. Usually officials are afraid of acting too aggressively (and being accused of trampling basic rights and liberties), but when it appears an attack is imminent officials are afraid of acting too timidly (and failing to prevent the next strike). *See id.* During a crisis, the expected costs of hoarding—including psychic costs of shame, guilt, and sorrow, as well as the prospect that policymakers might adopt reforms that undermine an agency's influence and autonomy, *see infra* note 267, become greater than they ordinarily would be. This reversal in incentives may explain why intelligence officials were uncharacteristically (but perhaps still insufficiently) willing to share information during the 2001 "summer of threat." *See supra* notes 66–73 and accompanying text.

262 *See supra* Part I.A.1.

263 *See* Banks, *supra* note 3, at 1150 (arguing that the wall was attributable to "[a]n institutional tradition hostile to coordination" and that "laws were responsible" for the wall "only in a limited way"). *But see* 9/11 COMMISSION REPORT, *supra* note 2, at 79 (discussing numerous factors that impeded information sharing, including a misunderstanding of procedures issued by DOJ leadership); POSNER, SURPRISE ATTACKS, *supra* note 1, at 31–32 (discussing the various agency motivations and managerial failures that combined to limit information flow).

264 Gorelick Memo, *supra* note 25, at 2.

265 *See supra* Part I.A.1.

266 *See id.*

267 The possibility also exists that *hoarding* could undermine agency autonomy. Intelligence officials know that refusing to share information increases the likelihood that the government will fail to prevent a future surprise attack. That in turn increases the likelihood that Congress will order a comprehensive overhaul of the intelligence system, as after 9/11. And officials have good reason to fear that any such tinkering will interfere with their turf. For instance, CIA bore much of the blame for failing to prevent 9/11, and subsequent reorganizations eroded its autonomy. Not only did Congress designate the new Director of National Intelligence as head of the intelligence community, effectively demoting CIA in the process, but rival agencies like the Defense Department and the FBI raided CIA's turf with impunity. *See* POSNER, COUNTERING TERRORISM, *supra* note 171, at 43–44. Why, then, don't the fears of autonomy loss

III. What Can Be Done?

Parts I and II described how the federal government's principals have an interest in enhanced information sharing, but their agents decidedly do not. The challenge is to devise a set of new incentives that can solve the agency-cost problem by bringing intelligence agencies' interests into alignment with those of policymakers on Capitol Hill and in the White House. Equally important, any new pro-sharing incentives must not weaken agencies' existing incentives to produce intelligence in the first place; the weaker the incentives to prepare assessments, the fewer there will be.[268] If agencies' reluctance to share has something in common with problems that arise in the worlds of intellectual property, antitrust, and organizational theory, maybe those fields can offer insights on how to incentivize data exchange. Perhaps the solutions those disciplines have developed to deal with hoarding, collusion, and risk aversion in the private sector can be adapted for the context of public sector information sharing.

This is a good place for modesty. It's easier to diagnose the malady than to prescribe a cure, and some of the possible solutions are more feasible than others. The discussion that follows should not be understood as an endorsement of any particular remedy to the hoarding problem. My objective is simply to lay out a menu of possible options from which policymakers may wish to pick. This Part is intended as a deliberately provocative thought experiment: if intelligence agencies hoard information for the reasons suggested above, what sorts of policy solutions would follow? Another important caveat: I do not argue that sharing invariably is good in all circumstances. Sometimes agencies will be justified in withholding information—for example, when disclosure poses an intolerable risk of compromising a critical intelligence source or method.[269] The solution is not to compel data exchange in all cases, but rather to establish

---

from hoarding offset the fears of autonomy loss from sharing? The most likely explanation is that the expected per capita costs of sharing are much greater than the expected per capita costs of hoarding. If Congress reorganizes the intelligence community, the resulting costs (loss of turf, transition costs, etc.) will be diffused among each of the losing agency's employees; the costs may even be diffused among all agencies within the intelligence community. By contrast, the costs of sharing (transfer or termination, criminal sanctions, etc.) are borne directly by the agency officials who authorized it.

268 *Cf.* Banks, *supra* note 3, at 1193 ("It may make good sense to encourage greater cooperation and coordination of intelligence and law enforcement functions in response to the challenges posed by terrorism. These steps should be taken, however, without giving up the advantages of the specialization and rivalry between them.").

269 *See supra* note 12 and accompanying text.

mechanisms capable of sorting the restrictions that are justified from the ones that are not.[270] On occasion it will be appropriate to withhold. What matters is that the decision to do so should be insulated, to the greatest extent possible, from agencies' self-serving determinations about what will advance their own parochial interests.

A. Intellectual-Property Solutions

One solution that can be dismissed out of hand is to abolish intelligence agencies' property interests in information altogether.[271] Doing so would destroy agencies' incentives to gather information in the first place; it would result in significant commons problems.[272] Imagine a village whose council abolishes farmers' exclusive property rights in their respective lands and replaces them with community ownership of a single field. A rational farmer would invest only a minimal amount of effort, if any, in growing crops. The farmer would bear all the costs associated with producing food—plowing, sowing, harvesting, and so on—but the benefits of his toil could be appropriated by all the other villagers. If farmers can't internalize the benefits of their labor, the village will soon find food in short supply. The same goes for intelligence. In the absence of property rights, agencies would no longer capture benefits from their production of intelligence outputs. An agency would incur all of the costs associated with gathering, analyzing, and producing intelligence, but the benefits of its outputs would be distributed among other agencies that use the information. And that means the incentives for agencies to collect and prepare intelligence product would be considerably weaker, maybe nonexistent. Why would it ever be in CIA's interest to write intelligence reports if it had to bear the production costs but received no compensation—

---

270 *Cf.* Swire, *supra* note 1, at 952 (proposing a "due diligence checklist" for determining when sharing should and should not take place).

271 The former Vice-Chairman of the 9/11 Commission has faulted intelligence agencies for viewing information "as their property, rather than the property of the entire government, and the property of the American people." *Federal Support for Homeland Security Information Sharing: Role of the Information Sharing Program Manager: Hearing Before the Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment of the Comm. on Homeland Security*, 109th Cong. 24 (2005) (statement of Lee H. Hamilton, Former Vice Chair, National Commission on Terrorist Attacks upon the United States); *see also* WMD REPORT, *supra* note 2, at 29 (rejecting "the (incorrect) notion that information is the property of individual intelligence agencies, rather than of the government as a whole"); THIRD MARKLE REPORT, *supra* note 2, at 45 ("[T]here should therefore be an explicit statement of policy that originators or producers do not own or control the information they produce.").

272 *See generally* Harold Demsetz, *Toward a Theory of Property Rights*, 57 AM. ECON. REV. 347, 354–59 (1967).

monetary, psychic, or otherwise—for them? The inevitable result would be less, and lower quality, intelligence. Collectivization of intelligence would yield the same disastrous results as collectivization of farms.[273]

Yet if outright abolition of property interests is imprudent, it's nevertheless advisable to adjust the rights protected by the current intelligence system. In effect, the current trade-secrets regime could be scrapped and replaced with a system of hybrid intellectual-property protections. This new hybrid scheme would draw principally from patent and copyright; to a lesser extent, it also would look to the *sui generis* protections available to business assets that don't fit neatly into established IP categories, such as "hot news" and databases. Doctrinal purity isn't important; we're painting on a clean canvas, so we can pick and choose the most appropriate elements from each regime. The resulting hybrid system would revolve around two fundamental policy objectives: First, incentivize agencies to make their products available to as many competitors as possible. Second, minimize the ability of rival agencies to free ride on originators' products (or, to say something similar, ensure that originating agencies are adequately compensated when their bureaucratic rivals make use of their products).

How do we adapt IP institutions to create incentives for intelligence agencies to share? For starters, the system might extend protections to the widest possible range of informational assets. The system could recognize property rights not only in finished intelligence assessments (the polished reports prepared for senior executive branch policymakers), but also in the raw or unprocessed information out of which those products are fashioned (e.g., unanalyzed transcripts of intercepted phone calls).[274] A proposal for broad IP protections might

---

273 *Cf.* POSNER, UNCERTAIN SHIELD, *supra* note 7, at 17 (arguing that recognition of property interests in intelligence information "may be needed to impart adequate incentives to intelligence agencies to obtain good data and produce cogent analysis").

274 Finished intelligence assessments may be thought of, in copyright terms, as original works that "possess at least some minimal degree of creativity." Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 345 (1991); *see also* 1 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 2.01[B] (2009) (discussing the creativity requirement of copyright law). The creative element here consists of intelligence analysts assembling, synthesizing, and interpreting raw information, thereby yielding an entirely new work. The assessments also could be thought of, in patent terms, as "inventions" or "discoveries," though the analogy is less exact. An intelligence analyst typically discovers new realities about enemy intentions (al Qaeda plans to attack within the month), not new processes for use in producing assessments. *See* 1 DONALD S. CHISUM, CHISUM ON PATENTS § 3.01. (A more precise patent analogy would be an agency launching a new satellite capable of vacuuming up an unprecedented volume of international

appear counterintuitive. Protecting both finished assessments and the underlying raw facts would give agencies extensive rights to exclude, and that seems an odd premise on which to base an argument for expanded information sharing. Yet such broad protections seem necessary to preserve existing agency incentives to collect information and turn it into finished assessments; the absence of such property rights would result in the commons problems just described. Broad protections also seem an indispensable first step in incentivizing agencies to share. The more data that is eligible for protection, the more opportunities agencies will have to be compensated when rivals make use of it. The availability of compensation helps offset agencies' natural tendency to hoard, and if the compensation is great enough may even overcome it. (Set aside for a moment the thorny questions of how to calculate the compensation due, and what forms it might take.)

Another way to sharpen pro-sharing incentives is to deny protection to intelligence product until the originating agency publishes it in some way. Such a publication requirement—the antithesis of trade secrets—would parallel the contemporary patent rule that an invention is not eligible for protection unless an application is filed with the Patent and Trademark Office ("PTO") (the PTO almost always publishes the application, thereby eliminating any trade secret protections).[275] The reason to make publication a precondition of property rights is fairly straightforward: it would give intelligence agencies powerful reasons to share. Indeed, it would flip the present incentive structure. Today, agencies see information as valuable only to the ex-

---

telephone calls, or placing a new spy whose reports offer exceptionally clear insights into the target's plans.) Unprocessed information doesn't fit as neatly into an established IP category; "facts are not copyrightable." *Feist*, 499 U.S. at 344. Yet these raw, unadorned facts resemble other types of information that enjoy what are known as *sui generis* IP protections. For instance, they are similar to "hot news," first recognized in *International News Service v. Associated Press*, 248 U.S. 215, 235–39 (1918). Like hot news, an intelligence agency gathers raw facts "at a cost," the data "is time sensitive" (an indication that a terrorist attack is imminent isn't much use after the bomb goes off), the agency directly competes against rivals that might free ride on its efforts, and such free riding might reduce or even eliminate the incentives to produce assessments. Nat'l Basketball Ass'n v. Motorola, Inc., 105 F.3d 841, 845, 852 (2d Cir. 1997). Raw facts also resemble the bulk information that, in Europe, is subject to a new type of IP protection known as "database right." *See* Council Directive 96/9, 1996 O.J. (L 77) 20, 25–26 (EC). That right protects firms that make a "substantial investment" in preparing the contents of a database against commercial rivals who "extract[ ]" or "re-utiliz[e]" database information for their own operations. *See id.* art. 7(1), at 25. Whatever the appropriate IP analogies, the basic point is simple: finished assessments and raw data both should be protected under a hybrid system.

275 *See* 35 U.S.C. § 122(b)(1)(A) (2006); 3 CHISUM, *supra* note 274, § 7.01 (pointing out that, on publication, "the patent immediately increases the storehouse of public information available for further research and innovation").

tent that others are denied access to it. In a world with a publication requirement, agencies would enjoy no IP protection if they kept their product to themselves—and, more to the point, they would not be entitled to any compensation for rivals' use of their information. (Again, set aside the obvious compensation questions for the time being.)

A publication requirement might be translated into the national security context by creating a register of intelligence products, akin to the PTO's primary register. In other words, there could be a central clearinghouse for all of the federal government's intelligence information (similar to the National Counterterrorism Center[276] and, as it was originally conceived, the Department of Homeland Security[277]). Another possibility is interactive publication—the originating agency could post information to a wiki-based web page where analysts from other agencies can access and comment on it. (The intelligence community is experimenting with these tools, such as the "CIA Wiki" and the DNI's "Intellipedia."[278]) Or, instead of insisting that agencies publish the underlying information, they could be required to prepare capsule summaries for inclusion in a searchable index. Analysts throughout the intelligence community would be able to search the index and, if they find an entry that might be useful, ask the custodian for access to the underlying information.[279] Once publication has been accomplished (in whatever form), the originating agency would be qualified to receive compensation when its product is used by another. A publication requirement also could create favorable incentives at the level of individual officers. The President could instruct the DNI not to include in the President's Daily Brief any intelligence reports that have not been published. Because analysts strive to make it into the PDB, such a policy would strongly incentivize them to comply with the publication requirement.[280]

---

276 *See supra* notes 135–39 and accompanying text.

277 *See supra* notes 120–22 and accompanying text.

278 David E. Kaplan, *Wikis and Blogs, Oh My!*, U.S. NEWS & WORLD REP., Nov. 6, 2006, at 52, 52–53.

279 *See* FOURTH MARKLE REPORT, *supra* note 2, at 11–14.

280 A publication requirement might run into significant obstacles. For starters, broad distribution of the underlying data might compromise sensitive sources and methods. A PTO- or wiki-style clearinghouse presents another danger: the consequences of a hack or other security breach are more dire if the information is warehoused in a single location than if it is stored throughout a decentralized network. "Such a database would be like a ship without bulkheads." POSNER, COUNTERING TERRORISM, *supra* note 171, at 84. Publication of capsule summaries in a searchable index probably poses fewer risks.

A compulsory licensing scheme is another IP mechanism that could ensure widespread dissemination of intelligence product. Under copyright law, a would-be user of certain musical pieces, television programs, and other works can effectively force the copyright holder to grant it a license to use the work in exchange for royalties.[281] As a result, works are widely disseminated that otherwise might have been closely held, as authors are unable to pursue holdout strategies and refuse to participate in transactions that would enhance net social welfare. Compulsory licenses might have a similarly beneficial effect in the intelligence context. They would enable an agency that wishes to use and incorporate a rival's work product into its own assessments to do so without dickering over terms, provided only that it pays adequate royalties to the originator. Compulsory licenses thus would modify the broad IP protections offered to various types of agency informational assets. Intelligence agencies would enjoy sweeping protections not only in finished assessments but also in raw data, but they would come with strings attached: agencies would be obliged to hand over much of that information to their competitors.

Of course, it's not enough simply to require intelligence agencies to share their outputs with their bureaucratic rivals. Such a requirement does nothing to solve, and even exacerbates, the free-riding problems that characterize the current system. This brings us to the second fundamental policy consideration: any IP scheme for intelligence must include a robust compensation mechanism. A recipient agency should not be able to free ride on the creative efforts of an originator; it should not be allowed "to reap where it has not sown."[282] Originating agencies should receive royalties for the same reason that inventors and artists are given temporary rights to exclude—not so much because they deserve it in a moral sense, but because of more utilitarian considerations.[283] Compensation helps ensure that agencies that produce useful intelligence assessments are able to internalize some of the benefits accruing to rivals that make use those products, thereby preserving incentives to prepare assessments in the first place.[284]

---

281 *See* 2 NIMMER & NIMMER, *supra* note 274, § 8.04, 8.23[A][1].

282 Int'l News Serv. v. Assoc. Press, 248 U.S. 215, 239 (1918).

283 *But see generally* Eric R. Claeys, *Property 101: Is Property a Thing or a Bundle?*, 32 SEATTLE U. L. REV. 617, 631 (2009) (book review) (arguing that property rights are based in part on moral desert); Adam Mossoff, *What Is Property? Putting the Pieces Back Together*, 45 ARIZ. L. REV. 371, 439–43 (2003) (same).

284 Our system of hybrid IP rights should reject the fair-use doctrine, under which a qualifying user may use a copyrighted work without being deemed to have infringed the copyright. *See*

Notice the implicit assumption of the previous paragraph: the remedies available to agencies whose products are used by rivals should be limited to something like money damages, and should not include quasi-injunctive relief ordering the competitors not to use the information. In other words, an agency's hybrid IP protections should be secured by a liability rule, not a property rule.[285] A liability rule would ensure that an agency would not be able to categorically bar a rival from making use of its product. Instead, the originator would simply be entitled to royalties from the infringer. The result is that the originating agency receives full compensation for its product (thereby preserving incentives to produce intelligence in the first place), but the system also ensures that the originator cannot impose obstacles to the distribution of potentially helpful intelligence.

Creating a workable compensation scheme is easier said than done. We are rapidly approaching the limit at which the analogy between intelligence and intellectual property becomes intolerably strained. One possible form of compensation would be for the recipient agency to provide the originator with a share of the enhanced budgetary outlays resulting from any intelligence breakthroughs the recipient makes as a result of the originator's information. The shortcomings should be fairly obvious. First, an agency's budget typically reflects an aggregation of various successes and failures over the course of months if not years, so it's not always possible to isolate the portion of the budget that corresponds to a particular intelligence breakthrough. More fundamentally, a share of the recipient agency's budget is not likely to fully compensate the originator for the use of its information. The originating agency also would need to receive a share of the recipient's nonmonetary profits, such as its enhanced prestige and, therefore, more secure turf and expanded influence over senior decisionmakers.

It is exceedingly difficult to devise a profit-sharing mechanism by which an originator might capture a portion of the recipient's newfound influence and autonomy. One way would be to insist that the breakthrough intelligence assessment give appropriate credit to the originator for providing the piece of information that proved to be the silver bullet—for example, a footnote. Yet an originating agency is

---

4 NIMMER & NIMMER, *supra* note 274, § 13.05. Allowing a recipient agency to make uncompensated use of another's intelligence product would enable it to transfer to itself profits that properly belong to the originator.

285 *Cf.* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1092 (1972).

unlikely to regard a footnote as adequate compensation to offset its loss of relative influence and autonomy.[286] The originator likely will fear that an isolated footnote is going to escape decisionmakers' notice. Also, footnote references to other agencies' assessments are already common features of intelligence reports. Despite that, agencies still hoard, which is a pretty good sign they regard footnotes as inadequate compensation. Another way to try to capture a share of the recipient's nonmonetary profits is for the originator to be rewarded with co-author status of the breakthrough report. Prominent recognition might succeed in diverting to the originator an adequate share of the recipient's prestige, but that raises problems of its own. What if not one, but ten agencies provided information that collectively resulted in the intelligence breakthrough? It would be unwieldy to list all ten as co-equal authors. Not only that, but if all ten received co-authorship the per capita value to them of that recognition would diminish. The lower an originating agency's per capita share of prestige, the less it is likely to regard the compensation as adequate. So it seems there is no neat solution to the problem of compensating intelligence agencies for others' use of their information.

Or maybe there is. This brings us to the most provocative reform implied by the intellectual-property framework: policymakers might consider establishing a market in which agencies are able to buy and sell particular pieces of information—not in a metaphorical sense, but for actual cash.[287] One advantage of a market-based solution is its simplicity. The various different forms of compensation an originating agency might demand—a share of budgets, a footnote, co-author status, and so on—could be reduced to a single form: money. A market system thus would help mitigate (though probably not eliminate; more on this in a moment) the valuation problems associated with compensating an agency for a rival's use of its intelligence outputs. Agencies would simply monetize the purchasing agency's expected influence and autonomy profits, and the selling agency's expected losses, and

---

286 For similar reasons, the remedies envisioned by hot-news protection are unlikely to fully compensate an intelligence agency for a rival's use of its product. Under the hot-news doctrine, a firm whose competitor free rides on its compiled facts is entitled to fairly modest forms of relief. The free rider might be forced to acknowledge the source of the information (e.g., INS would need to attribute its stories to the AP), or it might be required to delay publication for a period of time (e.g., INS would need to wait four hours before publishing AP-derived stories on the west coast). *See Int'l News Serv.*, 248 U.S. at 241–42.

287 *Cf.* BRUCE D. BERKOWITZ & ALLAN E. GOODMAN, BEST TRUTH: INTELLIGENCE IN THE INFORMATION AGE 122 (2000) ("A flexible, decentralized intelligence community managed through market-like mechanisms is better suited to the new environment.").

build them into the sale price. Another advantage of a market solution is its superior accuracy. Just as the price system associated with the free market typically is the most effective way of routing societal resources to their most productive uses,[288] so agencies presumably are in the best position to quantify how data exchange is likely to affect their respective bottom lines. (They certainly are better equipped than a law professor.)

That suggests an obvious drawback of an intelligence market. For such a system to work, agencies would be need to be able to predict, ex ante, the value that a particular piece of information would have to the recipient's intelligence assessments, as well as the magnitude of the profits (monetary and otherwise) the recipient stands to gain from any resulting intelligence breakthroughs. As I have suggested, there are reasons to doubt that agencies are capable of making these predictions.[289] The seller agency would know how the information benefits its own intelligence products, but not the buyer's products. The buyer in turn would only know the bare minimum about the information—its general subject matter, the persons it concerns, etc.—and so would not be able to say how the unknown information would benefit its intelligence products. Besides, how do you monetize influence and autonomy?[290] Another shortcoming is less theoretical and more practical. Policymakers have shown little appetite for using market-based solutions to solve intelligence problems. A proposal by the Defense Advanced Research Projects Agency to create a "terrorist futures market" to aid in the prediction of surprise attacks was quickly scuttled after several members of Congress denounced it.[291] Although an intelligence market is concededly provocative, it might be worth considering if only because it may spur creative thinking about other possible solutions to the problems of data exchange and compensation.

B. Antitrust Solutions

The intelligence system presently lacks, and would benefit from, a robust enforcement mechanism to promote information sharing and resolve sharing conflicts among intelligence agencies. Federal anti-

---

288 *See* F.A. Hayek, *The Use of Knowledge in Society*, 35 AM. ECON. REV. 519, 526 (1945).

289 *See supra* notes 170–73 and accompanying text.

290 *Cf.* POSNER, UNCERTAIN SHIELD, *supra* note 7, at 148 ("A government agency does not produced a monetized or readily monetizable output.").

291 *See* Carl Hulse, *Congress Shuts Pentagon Unit over Privacy*, N.Y. TIMES, Sept. 26, 2003, at A20; Carl Hulse, *Pentagon Prepares a Futures Market on Terror Attacks*, N.Y. TIMES, July 29, 2003, at A1; *see also* RICHARD A. POSNER, CATASTROPHE: RISK AND RESPONSE 175–76 (2004) (arguing that information markets are unlikely to reliably predict terrorist attacks).

trust law uses a suite of elements to prevent anticompetitive conduct and promote consumer welfare—centralized regulation and enforcement by administrative agencies,[292] private enforcement through civil lawsuits for money damages,[293] and private ordering that harnesses market forces. Policymakers might deploy a similar set of mechanisms to dissuade intelligence agencies from hoarding and create new incentives to share.

Congress already has recognized the need for something like a central regulator to oversee the intelligence community's data-exchange efforts. The program manager ("PM") of the Information Sharing Environment, whose office was established in 2004, is broadly assigned "responsib[ility] for information sharing across the Federal Government."[294] The PM thus is a rough counterpart of the two federal agencies charged with enforcing the nation's antitrust laws: the Justice Department's Antitrust Division and the Federal Trade Commission.[295] But only a rough counterpart—his powers are weak to the point of nonexistence. Although the PM in theory has authority to establish federal information-sharing policy,[296] he has no real investigative or enforcement authority. Private firms that violate the antitrust laws face the prospect of hefty civil fines as well as criminal sanctions.[297] But these sanctions have no counterparts in the intelligence world. An intelligence agency can persist in hoarding safe in the knowledge that its truculence won't interfere with its bottom line or those of individual employees. One obvious solution, then, is to bolster the PM's powers to investigate and punish violations of federal information-sharing policy. Policymakers might grant the PM express authority to monitor the performance of intelligence agencies, including through a subpoena-like power to demand access to hoarded intelligence assessments that other agencies are seeking to acquire. (Section 202 of the Homeland Security Act grants a similar power to the Secretary of Homeland Security.[298]) The PM could use his quasi-subpoena power to determine whether the hoarding agency was justified in holding back (e.g., because of the need to protect sensitive in-

---

292 *See* HOVENKAMP, *supra* note 209, § 15.1.

293 *See id.* § 16.1.

294 Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458 § 1016(f)(1), 118 Stat. 3638, 3667 (codified at 6 U.S.C. § 485(f)(1) (2006)).

295 *See* HOVENKAMP, *supra* note 209, § 15.1.

296 Intelligence Reform and Terrorism Prevention Act § 1016(f)(2)(A)(ii), 118 Stat. at 3668 (codified at 6 U.S.C. § 485(f)(2)(A)(ii) (2006)).

297 *See* HOVENKAMP, *supra* note 209, § 15.1a–15.1b.

298 *See supra* notes 120–22 and accompanying text.

telligence sources and methods). If the answer is no, the PM could be authorized to give the information directly to the aspiring recipient.

Also, Congress might give the PM authority to impose monetary sanctions on agencies, subunits within agencies, and maybe even individual employees. An agency or subunit that is derelict in its information-sharing responsibilities might find its budget for the upcoming year slashed by a certain percentage. Less money means less ability to influence policymakers and less ability to pursue agency priorities. As for individual employees, those whose information-sharing performances are wanting might be denied promotions. (An even more extreme option is to dock the pay of underperforming employees, but the Fifth Amendment's Due Process Clause likely would require such a sanction to be accompanied by elaborate administrative and judicial procedures.[299] The resulting costs of administering the system may well offset the gains.) In addition to the stick, the PM might be given a bushel of carrots. The PM could offer monetary rewards to agencies, subunits, and employees whose commitment to information sharing is exemplary. Congress might appropriate a pool of money to pay for these cash bounties, or the PM might use the funds raised by fining the underperforming agencies. The latter is, in effect, a proposal for impoundment (in which the executive branch declines to spend funds appropriated by Congress) and reprogramming (in which the executive branch redirects appropriated funds from purposes specified by Congress to other purposes). It is unclear that the President has authority under the Constitution unilaterally to impound or reprogram appropriated funds,[300] so Congress may wish to enact a limited statutory authority to do so here.

Another public-enforcement mechanism that could be adapted to the information-sharing context is the Justice Department's corporate leniency policy.[301] Under that policy, private firms that have been complicit in anticompetitive conduct—such as participating in a price-fixing cartel—may report their partners to the authorities in exchange for immunity. Only the first firm to come forward is assured of immunity. The effect is to create a strong incentive to be the first mover;

---

299 *Cf., e.g.*, Bd. of Regents v. Roth, 408 U.S. 564, 576–77 (1972) (describing procedural due process requirements imposed by the Fourteenth Amendment in cases involving government employee benefits).

300 *See, e.g.*, Wm. Bradford Middlekauff, Note, *Twisting the President's Arm: The Impoundment Control Act as a Tool for Enforcing the Principle of Appropriation Expenditure*, 100 YALE L.J. 209 (1990).

301 U.S. Dep't of Justice, Leniency Program: Antitrust Division, http://www.usdoj.gov/atr/public/criminal/leniency.htm (last visited Oct. 2, 2009).

the policy creates a "race to the Antitrust Division." Policymakers might consider offering intelligence agencies a similar deal. Agencies that have made arrangements with their rivals to divide intelligence submarkets or otherwise hoard information would have an incentive to blow the whistle on other cartel members in exchange for assurances that the PM's sanctions will fall elsewhere. The PM thereby learns about hoarding arrangements that he otherwise might not have detected, and his enforcement costs are reduced.

The prospect of new penalties for hoarding, and new rewards for sharing, would alter the cost-benefit analysis for agencies and individual employees alike. An agency's expected costs of data exchange (the potential loss of influence and autonomy) would be countered by new sharing-related benefits and hoarding-related costs. In some circumstances, the new costs and benefits could prove decisive, tilting the balance in favor of sharing. Yet antitrust law's public-enforcement tools are unlikely to prove a complete solution.[302] In the private sector, DOJ and FTC antitrust enforcement is complemented by a parallel ability of private parties to bring civil lawsuits against violators for money damages.[303] Policymakers in the intelligence context might consider supplementing the public-enforcement mechanisms with a robust system of private enforcement—i.e., they might consider an internal litigation mechanism that agencies may use to challenge competitors' refusals to share.

A major advantage of private enforcement is that it offers a lower-cost way to detect and remedy information hoarding. Knowledge about agencies' data-exchange activities is distributed throughout the intelligence system; no one has total knowledge of which agencies are sharing and which are not. Instead, individual agencies have piecemeal knowledge about the ground-level data-exchange realities that pertain to them. Because this information is dispersed, it would be prohibitively expensive (maybe even impossible) for a single regulator to obtain the knowledge needed for effective enforcement.[304] Another related advantage of private enforcement is its effectiveness. Because of agencies' superior knowledge of information-sharing conditions, they may detect hoarding that would have gone

---

302 *Cf.* POSNER, SURPRISE ATTACKS, *supra* note 1, at 42 (arguing that "a high official, far removed from the operating level of the intelligence services," is unlikely to "get intelligence officers to share information if they don't want to").

303 *See* HOVENKAMP, *supra* note 209, § 16.1.

304 *Cf.* Hayek, *supra* note 288, at 519–20.

unnoticed if the system relied only on a central regulator.[305] (Of course, agencies will never have complete knowledge of the extent to which their rivals are hoarding. Many times, an agency will be unaware that a competitor has information that could enhance its analytical outputs. In those circumstances—when an agency doesn't know what it doesn't know—even private enforcement will be imperfect.)

The issue then becomes what form a private-enforcement scheme could take. Who should be responsible for adjudicating the complaints lodged by individual agencies? The obvious candidate is the PM himself. The PM thus would wear two hats, prosecutor and judge. He would be responsible for initiating his own investigations of hoarding (and punishing it), as well as adjudicating complaints brought by other agencies. Combining both responsibilities in a single officer would yield efficiency gains by decreasing the costs of administering the enforcement system. It also would allow for the liability standards to be harmonized between the public- and private-enforcement spheres, preventing different decisionmakers from reaching inconsistent conclusions about which types of hoarding are impermissible. Congress has resisted combining different administrative functions in a single agency official,[306] but it has used such an approach in other contexts. In immigration law, the Attorney General is both prosecutor and judge. He is responsible for deciding whether to file charges before DOJ's immigration judges, and also has responsibility for reviewing (and ultimately rejecting) the immigration judges' decisions.[307] It would be unusual to grant the PM power to investigate violations in his own right, and also to adjudicate alleged violations brought to his attention by others, but it wouldn't be unprecedented.[308]

---

305 This is not an argument that individual agencies have stronger incentives to detect hoarding than the PM. An agency obviously will have a strong interest in acquiring information that enhances its analytical products, and it therefore will have an interest in monitoring hoarding by rivals. But the PM has an equally strong careerist interest in making sure agencies have all the information they need; he will want to be seen by his superiors as someone who can get the job done.

306 *See, e.g.*, 5 U.S.C. § 554(d) (2006) (providing that "[a]n employee or agent engaged in the performance of investigative or prosecuting functions for an agency in a case may not, in that or a factually related case, participate or advise in the decision").

307 *See generally* 3 C.J.S. *Aliens* §§ 409, 479 (2003).

308 Another option would be to establish a multi-member board, whose members are drawn from the various intelligence agencies, and that would report to the PM (or directly to the DNI). Some agencies have begun to experiment with comparable mechanisms to adjudicate intramural information-sharing disputes. DHS has created the Information Sharing Governance Board, which, among other responsibilities, adjudicates complaints brought to it by DHS components (e.g., if Immigration and Customs Enforcement refuses to share information about an

Another question is whether the intelligence system's private-enforcement scheme should offer remedies akin to the ones available under antitrust law's private-enforcement scheme—i.e., money damages. It's not obvious that money damages are needed to spur disappointed agencies into challenging their competitors' decisions to hoard. Agencies will have a strong natural incentive to litigate against rivals that refuse to share. This is so because hoarding undermines the agency's acquisition of data to enhance its analytical outputs, which in turn undermines the agency's influence and autonomy. That natural incentive may well be strong enough on its own to ensure that agencies have adequate reason to operate as private attorneys general, in which case quasi-injunctive relief would suffice. If not, cash bounties could be offered to agencies that report information-sharing violations. Again, Congress could appropriate funds especially for the purpose of rewarding agencies that successfully challenge hoarding by rivals, or the PM could tap funds generated by fining the hoarders. There are, however, some downsides. The prospect of cash bounties may lead to frivolous litigation. Agencies might challenge information-sharing restrictions that are justified (e.g., refusals to share information about sensitive sources and methods, or because of necessary compartmentalization) and that, absent the added lure of cash bounties, would have been left alone. The result of the surplus litigation would be to increase the enforcement system's administrative costs; even worse, the plaintiff agency may prevail and obtain a ruling that compromises information security.[309]

We've seen that antitrust law's public- and private-enforcement models can be adapted to the problems of information sharing. What about a deregulatory approach? It would be a mistake to rely too

---

ongoing investigation with the Secret Service). *See* DEPARTMENT OF HOMELAND SECURITY, INFORMATION SHARING STRATEGY: SECURING THE HOMELAND THROUGH INFORMATION SHARING AND COLLABORATION 4 (2008), *available at* http://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf. An upside of the committee approach is that agency participation may increase the perceived legitimacy of its decisions. If agencies have a stake in the committee's operations, they may be less likely to regard its decisions as efforts by other agencies to harm their interests. A downside is that multiple member commissions increase the danger of logrolling. CIA may vote to sustain the NSA's refusal to share information in return for the NSA siding with CIA on a different issue. There is a danger that the collusion we see in the marketplace thus could be transplanted into the decisionmaking body charged with overseeing the marketplace.

309 Cash bounties also might amplify the yes-man effect—the occasional tendency of intelligence agencies to provide assessments that confirm policymakers' preconceptions. *See supra* notes 167–69 and accompanying text. Agencies' existing incentives to tell policymakers what they want to hear will only grow stronger if they stand to reap monetary rewards for doing so.

heavily on private ordering to produce greater levels of information sharing. The market for intelligence products is so distorted—it is characterized by monopsony, oligopoly, significant barriers to entry and exit, and agency dominance in submarkets—it seems inevitable that agencies will engage in anticompetitive conduct. A deregulatory approach also would be hampered by absence of a price system for intelligence products. In private markets, price sends important signals about the extents to which various commodities are valued, and those signals enable producers to reallocate resources to their most productive uses. Because intelligence information cannot be bought or sold for money (though it can be bartered), the intelligence system lacks an objective signal like price that can direct resources to their best uses. That shortcoming reduces the effectiveness of a pure system of private ordering. (The problems arising from the lack of price information could be overcome if intelligence agencies were allowed to buy and sell data, as discussed above.)

Yet it also would be a mistake to conclude that calls for antitrust deregulation have no relevance to information sharing. Policymakers might experiment with private intelligence analysis.[310] Private firms could be hired to review "open source" information—i.e., unclassified data that's available to the general public, such as newspaper articles—and produce assessments that would compete against outputs from mainline intelligence agencies.[311] One benefit of private intelligence is its effectiveness. In some circumstances, private-sector analysts may provide goods that not only are close substitutes for agency products, but are actually superior. In the final years of the Cold War, several private firms relied solely on open source information to conclude that the Soviet Union was drawing its last breaths. The intelligence community's assessments, based on classified data, were nowhere near as accurate.[312] Even more important, private firms would inject a measure of competition into the intelligence market. Incumbent intelligence agencies would find themselves vying with

---

310 This is not an argument for private *collection*, only private *analysis*. The use of private assets to gather data—such as through interrogation or electronic surveillance—raises very different problems than the use of private assets to analyze data that's already been gathered or that's publicly available. *See* Simon Chesterman, *'We Can't Spy . . . If We Can't Buy!': The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Functions'*, 19 EUR. J. INT'L L. 1055, 1064 (2008).

311 *See generally* POSNER, COUNTERING TERRORISM, *supra* note 171, at 72–81; James Q. Wilson, *Thinking About Reorganization*, *in* U.S. INTELLIGENCE AT THE CROSSROADS: AGENDAS FOR REFORM 28, 33–34 (Roy Godson et al. eds., 1995).

312 *See* COLL, *supra* note 44, at 159–60; DANIEL PATRICK MOYNIHAN, SECRECY: THE AMERICAN EXPERIENCE 190–94 (1998).

new entrants for policymakers' attention. The competitive pressures presumably would lead them to improve their intelligence products. Competition also would remedy at least some of the distortions in the current intelligence market. By reducing entry barriers, the use of private firms would make it more difficult for agencies to form and maintain intelligence cartels. Also, private firms would be able to undercut cartels that did manage to form, by selling their goods at lower prices. Agencies can't undercut each other because they take the price the President offers, but private firms could undercut by signing lower-price contracts.

This is not to say that fostering competition from private intelligence firms will improve information sharing, at least not directly. Agencies are reluctant to share with rivals in the intelligence community, and there is no reason to think they would be more eager to share with rivals in the private sector. For their part, private firms likewise will resist sharing their intelligence products with their public-sector counterparts. Sharing threatens to expose the firm's proprietary business information to competitors, both government and private sector. Plus, if agency acquires a private report and uses it to enhance its own products, chances are good that the firm's contract will be renewed at a lower price, or won't be renewed at all. But the use of private intelligence firms might make information sharing less necessary in the first place. Simply by increasing the volume of intelligence analysis, the use of private firms decreases the likelihood that some clue has managed to fall through the cracks. Private intelligence thus may be a substitute for information sharing.

It's necessary to emphasize the limits of antitrust remedies to hoarding problems. Antitrust-style enforcement mechanisms may dissuade intelligence agencies from refusing to deal with their rivals, and they may frustrate collusive market-division arrangements. But they won't prevent rent seeking: agencies that are determined to hoard will still find it in their interest to petition senior policymakers for monopoly rents. Indeed, if refusals to deal and collusion are outlawed, there may be a substitution effect; agencies may rent seek with even greater vigor than they presently do. Furthermore, the ultimate success of these enforcement mechanisms will depend on the PM's topcover. If the President and DNI are indifferent—or, worse, openly hostile—to his efforts to hold hoarders' feet to the fire, the PM will lack the political capital needed to take such radical steps as cutting budgets and redirecting funds. Heads of powerful agencies that are threatened by the PM's enforcement efforts will go over his head and get the Presi-

dent to order him to back off. There are no obvious structural solutions to these problems. Enforcement will be effective only if the PM's superiors are committed both to the overall information-sharing project and to the specific steps the PM takes to bring it about.

C. Organizational-Theory Solutions

Intelligence agencies resist information sharing in part because their rank-and-file employees are conditioned by an institutional culture of risk aversion. That aversion stems from the fact that the expected costs of sharing almost invariably are greater than the expected benefits. An individual employee has little to gain from sharing with a competitor and much to lose, including blame for his agency's resulting loss of influence and autonomy and maybe even criminal liability. The intelligence system lacks tools for managing those risks. The trick, then, is to "think through exactly what operating culture we wish to produce among rank-and-file employees and then design an organizational structure that will increase the chances of that culture being created and sustained."[313] One obvious way to promote a culture of information sharing is for senior officials in the executive branch—especially the President—to make data exchange a priority.[314] Even more important, new mechanisms are needed that can counter intelligence analysts' natural (and rational) risk aversion and create new incentives to engage in sharing that is risky yet desirable. In particular, we would want to increase the benefits a given analyst could expect to gain from sharing with a rival agency while decreasing the expected costs of doing so.

We've already discussed one mechanism that could magnify the expected benefits of information sharing: the program manager of the Information Sharing Environment could offer cash rewards to analysts throughout the intelligence community who are exemplary sharers. In addition to one-off cash bounties, the PM also might be authorized to reward high-performing employees with raises, promotions, reassignments to more prestigious positions, and other career benefits. The only other observation to add at this point is that the cash bounties and other rewards would need to be fairly substantial—large enough to offset an employee's anticipated costs from sharing,

---

313 Wilson, *supra* note 311, at 30; *see also* Banks, *supra* note 3, at 1172 (calling for "[r]eforms of the institutional culture" to resolve "problems of coordination and cooperation" among intelligence agencies).

314 *Cf.* Bibas, *supra* note 149, at 142 ("Culture is not easy to gauge from the outside, let alone regulate, but charismatic leadership can lead to change.").

which as we've seen are significant. An employee would need a lot of money to counterbalance the prospect that blame will damage his career prospects or even end his career altogether. Still more would be needed to offset the chance that sharing will expose him to criminal liability, as well as the significant attorneys' fees he might incur in the course of his defense. If the PM is able to offer sufficiently great benefits to intelligence analysts who share information—i.e., if the expected benefits of sharing are greater than the expected costs—then the present incentive structure will be reversed. Rational agency employees will stop hoarding and start sharing.

Adjustments would need to be made on the cost side of the ledger, as well. Cost is equal to the magnitude of the harm discounted by the probability that it will materialize. Reformers therefore could minimize the expected costs of information sharing by reducing the magnitude of the harms that sharing threatens to produce, or by reducing the probability that those threatened harms will occur. Or they could do both. This Article has already discussed one step that would reduce (or even eliminate) the costs an employee might bear as a result of information sharing—i.e., establishing an IP-type compensation mechanism by which agencies are reimbursed when rivals make use of their intelligence information. No harm is likely to befall an employee who authorizes the sharing of information if the originating agency is adequately compensated for the influence and autonomy it loses as a result. If there's no injury, there's no blame to be assigned.

Mitigating the expected costs of criminal liability would take a bit more work. For starters, Congress could consider legislation that modifies the criminal sanctions that might apply to employees who share information with colleagues in other agencies—e.g., the Trade Secrets Act, the Posse Comitatus Act, and so on. One option would be to simply repeal the penalties altogether and replace them with a system of civil sanctions aimed at the agencies themselves rather than at individual employees. To the extent that Congress deems the threat of criminal sanctions necessary to deter undesirable action—e.g., agency employees profiting from strategic leaks of one company's trade secret to a competitor, or members of the armed forces walking a beat like local police—it could simply carve out exceptions to the general criminal prohibitions for activities related to information sharing. Removing the prospect of jail time and fines would decrease the magnitude of the harms intelligence officials expect to face as a result of sharing. Another way to reduce the expected costs would be for Congress to eliminate the legal ambiguities that continue to cloud in-

telligence officials' judgment. Congress could enact new laws establishing bright-line rules that precisely clarify which sorts of coordination and sharing are permissible and which are not. The precise content of the rules may be less important than the fact that they exist. Even if Congress enacts legislation that rules certain kinds of sharing out of bounds, the effect of a law that eliminates ambiguities still may be to increase the volume of data that is exchanged.

In the absence of congressional action, lawyers in the executive branch might provide more guidance to intelligence officials about what sorts of information sharing would run afoul of the various statutory restrictions on interagency coordination. If agency officials rely on a definitive legal opinion rendered by an executive branch lawyer, they might enjoy qualified immunity even if a court later determines that the sharing was unlawful. In effect, the lawyers would be handing the analysts "get-out-of-jail-free cards."[315] The question then becomes which entity should have responsibility for interpreting the reach of sharing statutes. An obvious candidate would be the PM's office, but it may be inadvisable to foist this responsibility on it. The PM's job is to promote information sharing. His conclusion that a particular instance of data exchange is legally permissible is unlikely to be regarded as disinterested legal advice, and for that reason it may be risky for intelligence officers to rely on it. Perhaps the best candidate would be the Justice Department's Office of Legal Counsel ("OLC"), which traditionally is responsible for issuing legal interpretations that bind the executive branch. Because OLC is likely to be perceived as more disinterested than the PM's office when it comes to the legality of information sharing, its conclusion that a particular instance of data exchange is permissible will have more weight, and thus will offer agency employees stronger assurances of immunity.[316]

Reformers also might steal a page from the academic playbook. Not all producers of information have incentives to hoard. Scholars routinely share with colleagues, even those with whom they compete (for grants or professional prestige, for example). The reason is because they have strong careerist reasons to do so. An academic's ability to advance depends in part on his citation count—the number of other scholars who cite his work and the prestige of the journals in which those citations appear. In the academic world, sharing has low expected costs and high expected benefits. If a young law professor sends an article to a senior counterpart at Harvard, the worst that can

315 GOLDSMITH, *supra* note 244, at 96.

316 *See id.* at 96–97.

happen is that the reprint is thrown away unread. The potential upside, however, is enormous. The luminary might take an interest in the new professor's work and reference it in his own scholarship. In the intelligence community, the career incentives are opposite. An analyst who shares information with a colleague at a rival agency has much to lose (blame for any resulting harm to the agency's interests, not to mention the prospect of criminal liability) and very little to gain. Policymakers could look for ways to reverse these incentives and foster a quasi-academic culture of sharing within the intelligence community.

In particular, intelligence analysts' job performance might be measured partly by the extent to which the assessments they prepare are relied upon by other analysts.[317] Not only would such a citation-count performance measure strengthen the incentives to produce high-quality assessments (high-quality intelligence reports presumably are more likely to be cited than low-quality ones), it also would create powerful incentives to share. Like a junior scholar, an intelligence analyst would only be able to advance in the profession if others cited his work, and he therefore would want to make sure they know his work exists. Some post-9/11 information-sharing initiatives have called for the use of performance measures to encourage sharing. For instance, President George W. Bush's 2005 guidelines for the Information Sharing Environment direct intelligence agencies to, among other things, "develop high-level information sharing performance measures."[318] The idea is sound but underdeveloped. Evaluating intelligence analysts specifically on the extent to which their peers cite their work may help foster an organizational culture in which there are strong careerist reasons to share.

Conclusion

Intelligence agencies aren't going to start sharing information just because Congress and the President say please. It's not enough to eliminate legal obstacles to data exchange. Nor will it work to call for a new "culture of information sharing" or otherwise exhort agencies to do a better job. Agencies hoard because it's in their interest to

---

317 *Cf.* POSNER, UNCERTAIN SHIELD, *supra* note 7, at 214 (arguing that individual "[c]ollectors and analysts who are evaluated by the number of times their data or analyses are cited will have an incentive to present their product in a form that enables it to travel as far as possible throughout the intelligence system," and that they "will be disinclined to . . . restrict dissemination beyond actual security needs").

318 ISE Guidelines, *supra* note 74, at 1878.

hoard. What's needed is for policymakers to systematically reform the intelligence system's incentive structure; they need to mitigate agencies' incentives to hoard information and replace them with new incentives to share. That's harder than it sounds, because any new incentives to encourage information sharing must not undermine agencies' existing incentives to collect, analyze, and produce intelligence in the first place.

Fortunately, Congress and the President don't have to write on a blank slate. The reluctance of intelligence agencies to share information resembles problems that arise with some frequency in the fields of intellectual property, antitrust, and organizational theory. Policymakers might look to those disciplines for suggestions on how to overcome hoarding problems.

Intellectual-property norms suggest that hoarding could be mitigated by abolishing the current trade-secrets regime and replacing it with a system of hybrid IP protections inspired by patent and copyright principles. In particular, agencies might be required to somehow publish intelligence data as a condition of receiving IP protections, and the data might be subjected to a compulsory licensing scheme that allows rivals more or less unfettered access. In return, agencies should be fully compensated when their competitors make use of their products; they should be able to internalize a portion of the positive externality that accrues to the rival agency. Antitrust solutions likewise have some promise. Policymakers might strengthen the hand of the central regulator—the program manager of the Information Sharing Environment—by giving him meaningful powers to enforce sharing policy and to punish violators, including in their wallets. They also could establish a private-enforcement scheme, which would allow individual agencies to litigate against hoarders when their efforts to acquire data are thwarted. Finally, reformers could adopt organizational-theory solutions to overcome intelligence agencies' cultural aversion to risk. Agencies that share might be offered cash bounties to offset the loss of influence and autonomy they expect to incur as a result of data exchange. Policymakers also might clear up the remaining ambiguities about the legality of sharing, either by legislation or by opinion from counsel. By increasing the benefits agencies expect to gain, and by decreasing the expected costs, such measures might tilt the balance in favor of expanded information sharing.