SHARE AND SHARE ALIKE: INTELLIGENCE AGENCIES, INFORMATION SHARING, AND NATIONAL SECURITY

Nathan Alexander Sales,
George Mason University School of Law

George Washington Law Review, Forthcoming

George Mason University Law and Economics Research Paper Series

09-24

This paper can be downloaded without charge from the Social Science Research Network at http://ssrn.com/abstract_id=1392917
Why don’t intelligence agencies share information with each other? This article attempts to answer that perennially vexing question by consulting public choice theory as well as insights from other legal disciplines. It begins by surveying arguments for and against expanded sharing, examples of sharing failures, and recent reforms intended to encourage sharing. Next, the article considers why intelligence agencies see information sharing as a threat to the various values they maximize, such as influence over senior executive branch policymakers and autonomy to pursue agency priorities. It then proposes a series of analytical frameworks that enrich our understanding of why agencies resist sharing: At times data exchange resembles an intellectual property problem, sometimes it looks like an antitrust problem, and sometimes it looks like an organizational theory problem. Finally, the article examines whether the solutions suggested by these other disciplines can be adapted to the problems of information sharing.
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 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, Congress 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.\(^6\) Yet despite a decade of effort, there is a widespread sense that information sharing is “going nowhere.”\(^7\) Why?

---


3 See, e.g., 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); 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”).


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
Because policymakers have failed to account for the iron law of agency self-interest. 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.8

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

Part I discusses the costs and benefits of information sharing. A principal advantage of sharing is that it enables intelligence agencies to better identify threats to the national security. By assembling individual tiles that by themselves reveal little, data exchange allows analysts to see the entire mosaic of enemy intentions. Sharing also allows agencies to specialize, producing efficiency gains that result in more and better intelligence product. Yet sharing comes at a cost. Data exchange can burden privacy interests. It also threatens to expose sensitive intelligence sources and methods. Sharing can flood intelligence analysts with troves of data, making it harder for them to separate the signal from the noise and reinforcing their preconceptions about hostile powers’ capabilities and intentions. Sometimes it can even prevent agencies from acquiring information in the first place; private firms and foreign governments may be reluctant to provide data if the recipient agencies can’t promise the information will be closely held.

In Part II, I recount 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 II then describes the major post-9/11 legislative and executive initiatives to correct these problems.

Part III 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

---

8 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”).
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 III 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 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. Intelligence 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, sharing can be a “career stopper.”

Part IV 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 focuses primarily on challenges associated with “horizontal” information sharing – the exchange of data among peers (e.g., between one

---

9 See Kris, supra note 1, at 501; see also 9/11 COMMISSION REPORT, supra note 2, at 79.
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. 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. TWO CHEERS FOR INFORMATION SHARING

The post-9/11 conventional wisdom is that information sharing is a good thing. Sharing enables officials to piece together the intelligence mosaic, an especially important task in conflicts with nontraditional adversaries like terrorist organizations. Also, an intelligence system based on information sharing allows agencies to specialize, thereby producing efficiency gains. So why only two cheers? Because data exchange imposes costs on the persons to whom the information pertains, as well as on the agencies that are doing the sharing. Still, the costs associated with information sharing are often overstated, and sometimes there are ways to minimize the costs that do not involve erecting barriers to data exchange.

The principal benefit of information sharing is that it better enables intelligence analysts to detect threats against the United States. Taken individually, particular pieces of information might not reveal anything about an adversary’s intentions or capabilities. But seemingly innocuous data points can become more meaningful, and more sinister, when aggregated with other information. This is the mosaic theory. “[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.”

10 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. See infra notes 39 to 42 and accompanying text. 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 fail. The suspect may flee, and the camp may relocate. See Nathan Alexander Sales, Secrecy and National Security Investigations, 58 ALA. L. REV. 811, 821 (2007).


12 J. Roderick MacArthur Found. v. FBI, 102 F.3d 600, 604 (D.C. Cir. 1996) (quoting In re United States, 872 F.2d 472, 475 (D.C. Cir. 1989)); see also United States v. Marchetti, 466 F.2d 1309, 1318 (4th Cir. 1972) (“The significance of one item of information may frequently depend upon knowledge of many other items of information. What may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context.”).
mosaic might. Mosaic concerns are what led the Supreme Court in *CIA v. Sims*\(^{13}\) to uphold CIA’s refusal to reveal the identities of private researchers working for the agency. The petitioners had filed a request under the Freedom of Information Act seeking access to records about MKULTRA, a CIA project that funded private research into “chemical, biological, and radiological materials capable of employment in clandestine operations to control human behavior.”\(^{14}\) Why should CIA be allowed to withhold information that the Court conceded was “innocuous”?\(^{15}\) Because “bits and pieces of data ‘may aid in piecing together bits of other information even when the individual piece is not of obvious importance in itself.”\(^{16}\) Traditionally, the mosaic theory has been offered as reason why the government might resist the release of a particular piece of information. Yet while courts often treat it as a theory of nondisclosure, the mosaic theory also can be understood as a theory of intelligence analysis. For instance, General George Washington – “America’s first spymaster”\(^{17}\) – subscribed to it during the Revolutionary War: “Every minutiae should have a place in our collection, for things of a seemingly trifling [sic] nature when conjoined with others of a more serious cast may lead to very valuable conclusions.”\(^{18}\)

A related benefit of information sharing is that it can reduce the risk of intelligence failures that lead to sneak attacks, faulty analysis, and other harms. “[T]he intelligence failures that hurt the worst have not been those of collection but rather those of dissemination.”\(^{19}\) For instance, some scholars believe that shortcomings of information sharing contributed to our failure to anticipate the attack on Pearl Harbor. In the months before December 1941, American cryptanalysts had broken the principal code for Japan’s diplomatic communications (“MAGIC”) and intercepted a number of increasingly alarming messages that Japan regarded military conflict with the United States as inevitable.\(^{20}\) Intelligence officers also determined that Japan had changed its naval call signs on November 1 and again on December 1, which were regarded “as signs of major preparations for some sort of Japanese offensive.”\(^{21}\) Yet these and other alarming clues about Japan’s possible intentions were never pooled and integrated:

> [N]o single person or agency had at any given moment all the signals existing in this vast information network. The signals lay scattered in a number of different agencies; some were decoded, some were not; some traveled through rapid


\[^{15}\] Id. at 178.

\[^{16}\] Id. (quoting Halperin v. CIA, 629 F.2d 144, 150 (1980)).


\[^{21}\] WOHLSTETTER, *supra* note 20, at 385.
channels of communication, some were blocked by technical or procedural delays; some never reached a center of decision.\textsuperscript{22}

Likewise, the intelligence failures that contributed to the 2003 decision to invade Iraq were partly the fault of inadequate information sharing. The intelligence community’s prewar assessment that Saddam Hussein had biological weapons was largely based on a single human source – an Iraqi defector to Germany, code-named “CURVEBALL.” By late 2002, CIA had begun to doubt his reliability and it shared its skepticism with the Defense Department.\textsuperscript{23} But those doubts apparently were not communicated to senior policymakers, nor were policymakers told that the intelligence community’s assessment about Iraqi WMD was based almost entirely on CURVEBALL – a breakdown in vertical information sharing.\textsuperscript{24} It hardly needs to be said that CURVEBALL turned out to be badly mistaken.

Information sharing also pays dividends by allowing agencies to specialize, thereby producing efficiency gains that can result in more, and higher quality, intelligence product.\textsuperscript{25} Consider the alternative – a system in which agencies only gain access to data they manage to collect on their own. Such an “eat what you kill” regime would result in wasteful redundancies, as agencies duplicated each others’ collection capabilities. Resources that the FBI might use more productively to gather other kinds of data would be diverted to replicating the NSA’s signals-intelligence assets. Those inefficiencies mean less intelligence would be produced. (This is not a mere hypothetical. Agencies sometimes cope with sharing restrictions by developing their own redundant collection capabilities.\textsuperscript{26}) By contrast, an intelligence system based on information sharing allows agencies to specialize. Agencies can focus their collection efforts on areas where they enjoy a comparative advantage – e.g., the FBI’s comparative advantage in gathering information relating to domestic crimes, and CIA’s comparative advantage in gathering data from overseas spies. Sharing ensures that agencies won’t be disadvantaged by specializing; they will still (through a system of trade) have access to data collected by others. The result is to lower the intelligence system’s overall costs of producing assessments.

A related advantage is that information sharing fosters “all source intelligence,” resulting in better advice to policymakers. All-source analysis is based on data from many different collection sources, not just information the agency in question has gathered on its own.\textsuperscript{27} Sharing allows analysts to examine the widest possible range of data, including data gathered by

\textsuperscript{22} WOHLSTETTER, supra note 20, at 385. \textit{But see} David Kahn, \textit{The Intelligence Failure of Pearl Harbor}, FOREIGN AFFAIRS, Winter 1991-1992, at 138, 148 (“The intelligence failure at Pearl Harbor was not one of analysis, as Wohlstetter implies, but of collection.”).

\textsuperscript{23} WMD REPORT, supra note 2, at 89.

\textsuperscript{24} WMD REPORT, \textit{supra} note 2, at 93-94, 103-04, 177-80. \textit{But see} MARK M. LOWENTHAL, INTELLIGENCE: FROM SECRETS TO POLICY 311 (4th ed. 2009) (suggesting that the Iraq intelligence failure was the result of \textit{too much} sharing; “the lesson of Iraq WMD is to be careful and not share information that is dubious, such as the discredited reporting of the human source known as CURVEBALL”).

\textsuperscript{25} \textit{Cf.} POSNER, SURPRISE ATTACKS, \textit{supra} note 1, at 14, 47 (\textit{__}).

\textsuperscript{26} See infra note 100 and accompanying text.

\textsuperscript{27} See LOWENTHAL, \textit{supra} note 24, at 72.
other agencies. The result is a system of competitive analysis, in which multiple agencies consult a common pool of underlying data to tackle the same intelligence questions. At present there are just three all-source agencies – CIA, the Defense Intelligence Agency, and the State Department’s Bureau of Intelligence and Research;28; sharing could enable others to emerge. The previous paragraph argued that redundant intelligence collection is inefficient, but not all redundancy is wasteful; cars come equipped with seat belts and air bags, and drivers are safer for having them both. Redundant collection seems the very essence of waste; little is gained when five different agencies intercept the same phone call. But redundancy in intelligence analysis can be beneficial. Competitive analysis helps ensure that policymakers are exposed to diverse perspectives; it also helps to counteract groupthink tendencies.29

Information sharing may produce even greater benefits in conflicts with terrorists than in traditional warfare between nation states.30 Indications that a conventional attack is imminent are comparatively easy to detect. The warning signs of a terrorist attack are more difficult to spot. They could be as innocuous as an Algerian citizen taking a ferry from Vancouver to Washington state. In other words, it’s fairly easy to figure out what the Soviets have in mind when they mobilize 20,000 tanks to the border of West Germany, but terrorist attacks and other forms of asymmetric warfare often involve precursor acts that by themselves appear innocent.31 Their sinister implications can only be discerned when they are integrated with other pieces of information – e.g., indications that the ferry passenger (Ahmed Ressam, on his way to bomb LAX in connection with the millennium celebrations) had traveled to Afghanistan and was roommates with a member of an Algerian terrorist group.32 Information sharing enables intelligence analysts to cross-check seemingly innocent facts against other signs of possible danger, thereby approaching the comparative certainty of conventional threat assessments.

Information sharing offers a number of national-security benefits, but it’s not a cure all. As Judge Richard Posner has emphasized, many factors other than hoarding contribute to intelligence failures. Those factors include analysts’ cognitive biases (such as “interpret[ing] warning signs to fit a preconceived conception” of an enemy’s plans and disregarding other, more plausible, explanations for the alert), failure to comprehend an enemy’s intentions and capabilities, the “crying-wolf effect” of past false alarms, and so on.33 Even if data had flowed freely in the months before the 9/11 attacks – or Pearl Harbor, or the invasion of Iraq – it is far from clear that officials would have overcome these other obstacles to make the right intelligence

28 See Lowenthal, supra note 24, at 38.
29 See Banks, supra note 3, at 1151, 1193; Lowenthal, supra note 24, at 14, 139. Competitive analysis also has its downsides. “The existence of an alternative analysis, especially on controversial issues, can lead policymakers to shop for the intelligence they want or cherry-pick analysis, which also results in politicization.” Lowenthal, supra note 24, at 135.
30 See Swire, supra note 1, at 955-57.
31 See Lowenthal, supra note 24, at 133.
Enhanced information sharing may be necessary to stave off intelligence failures, but it is not sufficient. Just as sharing isn’t a snake-oil remedy capable of curing all intelligence failures, neither is it without its downsides. A system of widespread data exchange imposes costs. Those costs may not outweigh the benefits of information sharing, but they are still very real. For instance, sharing burdens the privacy interests of persons to whom the data relates. It’s fairly obvious that gathering data – through electronic surveillance, for example – imposes privacy costs. The sharing of previously collected data harms privacy in different ways. First, sharing increases the number of officials with access to an otherwise private fact; the more officials who observe that fact, the greater the privacy harms. Second, and more importantly, information sharing enables the government to integrate isolated units of data and thereby discover new information that it was never authorized to collect:

[W]hen combined together, bits and pieces of data begin to form a portrait of a person. The whole becomes greater than the parts. This occurs because combining information creates synergies. When analyzed, aggregated information can reveal new facts about a person that she did not expect would be known about her when the original, isolated data was collected.

The same insight informs the mosaic theory: Integrating isolated data points creates synergies, and those synergies effectively create new information. In the same way that data aggregation can reveal new insights into al Qaeda’s capabilities or plans, it can also reveal new insights into a person’s private thoughts and actions.

While information sharing can undermine privacy interests, an intelligence system based on data exchange has the potential to actually enhance privacy. This is so because sharing can be a substitute for surveillance. Sometimes the sharing of previously collected information will obviate need for further intelligence gathering. Imagine that Justice Department prosecutors have presented intercepted telephone conversations between two suspected terrorists to a grand jury. Analysts at CIA want to know what the two are up to. If CIA is able to acquire the intercepts from the Justice Department, it may not need to ask the Foreign Intelligence Surveillance Court to approve a new round of electronic surveillance to capture similar

---

34 See Lowenthal, supra note 24, at 256.
35 Contra Kris, supra note 1, at 520 (arguing that sharing restrictions “do[] not provide much protection for privacy”).
incriminating conversations. CIA will choose the existing intercepts over fresh surveillance if the expected benefits of doing so (conserving its scarce collection, translation, and analytic resources) exceed the expected costs (the risk that an additional round of surveillance will reveal new information not reflected in the existing intercepts). That means weaker burdens on targets’ privacy interests: They will only be subject to one wiretap, not two; and investigators therefore won’t need to listen to additional hours of personal and innocuous conversations in the hopes of discovering something relevant to the investigation. Information sharing thus has the potential to vindicate privacy interests to the extent it reduces officials’ need to collect more data.

Investigative targets aren’t the only ones who are potentially imperiled by information sharing. Sharing also has the potential to harm the government’s security interests. In particular, it can compromise sensitive sources and methods – “information about the manner in which the government collects intelligence,” such as the identities of spies, electronic-surveillance capabilities, and so on. And that enables surveillance targets to evade detection. Sharing thus can undermine the policy behind compartmentalization rules, “need to know” requirements, and other restrictions that protect the most sensitive intelligence secrets against espionage (acquisition by a foreign power) and leaks (disclosures to unauthorized persons, such as the news media). The greater the number of people who are privy to a secret, the greater the danger it will be exposed. “Bulkheads in a ship slow movement between the ship’s compartments, just as restrictions on sharing classified information slow the communication traffic between intelligence agencies. But in both cases there is a compelling safety rationale.”

Still, the risk that sharing might compromise sensitive data seems exaggerated. Cold War era information-access rules were designed to counter a particular type of threat – espionage by a traditional nation-state adversary like the Soviet Union – and they are less necessary in today’s era of asymmetric conflict. Sharing restrictions still play an important role as to data concerning rival nations, such as China or Russia. But terrorist groups like al Qaeda have not proven as adept at placing spies in the American intelligence community. At least as to information related to terrorist threats, then, the risks of espionage are weaker. Of course, the danger that terrorism-related information might leak remains significant – witness, for example, the steady stream of newspaper stories about the NSA’s warrantless Terrorist Surveillance Program, the existence of secret CIA prisons in Central Europe, and so on. But it might be possible to mitigate those risks with countermeasures other than sharing restrictions, such electronic audit trails that record which officials have accessed a particular piece of information.

38 See 50 U.S.C. § 1805(a) (authorizing the FISA court to issue an order approving electronic surveillance if it finds, among other things, probable cause to believe that the target is “a foreign power or an agent of a foreign power”). For a discussion of FISA, see Sales, supra note 10, at 839-49.

39 Sales, supra note 10, at 818; see also CIA v. Sims, 471 U.S. 159, 167 (1985) (describing sources and methods as “the heart of all intelligence operations”).

40 POSNER, SURPRISE ATTACKS, supra note 1, at 103.

41 Cf. POSNER, UNCERTAIN SHIELD, supra note 7, at 215 (indicating that, while “[f]oreign states have their own intelligence agencies that can steal secrets by pooling and analyzing scattered bits of information obtained from leaks or moles,” terrorist organizations “have much less elaborate intelligence apparatus,” and arguing that classifying information “is not responsive” to the threat posed by terrorists).

Another way data exchange can harm national security is by producing what might be called a “flooding effect” – i.e., by inundating analysts with massive amounts of information. Roberta Wohlstetter argues that intelligence analysis is akin to trying to locate a faint “signal” hidden amid a mass of “noise.” Information sharing can increase the amount of noise, making the signals even more difficult to detect. Sharing thus can overwhelm analysts, preventing them from detecting threats they otherwise would have found if only they weren’t swamped with data. Even worse, the flooding effect can lead to analytical distortions. By inundating analysts with unmanageable troves of data, sharing can reinforce their preconceptions about hostile powers’ capabilities and intentions and blind them to unexpected threats. In other words, sharing can produce confirmation bias. Analysts might cope with the massive amounts of new information by fixating on the data points that confirm their preexisting biases and ignoring the ones that don’t. The result is analytical ossification, as established theories are reinforced and unconventional assessments go unairied.

Concerns about flooding are legitimate, but they don’t justify wholesale limits on information sharing. It’s true that analysts’ cognitive limitations are an imperfect way to filter data. But so are sharing restrictions. In a system that uses sharing limits as a filter, what determines whether data from one agency reaches another is not an informed, disinterested judgment about whether or not it would be useful. Rather, the decisive factor is a rival agency’s self-serving determination about whether the exchange would benefit its interests or harm them. Sharing restrictions are an exceedingly coarse way to separate signal from noise. A better way to prevent analysts from being inundated with data might be to use automated technologies as filters. For instance, CIA reportedly is developing image-recognition technology that enables computers to match photographs with exemplars stored in a database. The Office of the Director of National Intelligence is experimenting with an automated system that can scan databases of foreign surveillance videos and identify suspicious behavior. And computers are often tasked with running keyword queries (“al Qaeda,” “jihad,” and the like) against intercepted phone calls and emails. Human beings would only need to inspect what passed the automated filters. Still, this seems an imperfect solution to the flooding effect. “Even in the age of computers, few technical shortcuts have been found to help analysts deal with the problem.”

A final way information sharing can harm national security is by preventing intelligence agencies from acquiring probative data in the first place. Sometimes foreign governments, private firms, and others will refuse to turn over information to an agency unless the recipient

---

43 *See* Wohlstetter, *supra* note 20, at 387, 393.

44 *Cf.* Wohlstetter, *supra* note 20, at 387 (“We failed to anticipate Pearl Harbor not for want of the relevant materials, but because of a plethora of irrelevant ones.”).

45 *See* Posner, *Surprise Attacks*, *supra* note 1, at 116-17.

46 *See* Lowenthal, *supra* note 24, at 73.


48 *Lowenthal*, *supra* note 24, at 117.
pledges to keep it closely held. These restrictions are known as ORCON, or “originator controls.” For instance, foreign officials sometimes provide data to the FBI only on the condition that the bureau not further disseminate it. (The foreign government might fear that further sharing would compromise its intelligence sources and methods, or would interfere with an ongoing investigation or prosecution.) Private industry might insist on similar limitations for similar reasons. A chemical plant might be willing to give DHS information about its facilities’ vulnerabilities, but only if the agency refrains from distributing the data any further. (The company might be concerned that publication of its vulnerabilities might invite an attack, or it might fear that rival firms could gain a competitive advantage by accessing its confidential business information.) Sharing restrictions thus may be necessary for the government to acquire the data in first place; an agency that refuses to commit to confidentiality might find that valuable pieces of information remain off limits. At the same time, there may be ways to accommodate these concerns without imposing limits on information sharing. Agencies can use electronic audit trails to find out who is accessing the information. And they can impose strict penalties to deter employees from misusing sensitive data (e.g., the Trade Secrets Act, non-statutory employment regulations, or terms of employment contracts).

II. 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 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 II 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

Perhaps the most notorious legal restriction on information sharing is the infamous “wall” between intelligence officials and criminal investigators. The wall – codified in a series of internal Department of Justice 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 the Justice Department. The USA PATRIOT Act set out to destroy the wall, and, with an assist

50 See LOWENTHAL, supra note 24, at 154.
51 Other walls exist. See infra notes 213 to 216 and accompanying text.
52 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. Later, the term
from a specialized federal appellate court, largely succeeded in doing so.\textsuperscript{53} Though the wall has come down,\textsuperscript{54} it remains a useful vehicle for understanding why administrative agencies are reluctant to share with one another.\textsuperscript{55}

The origins of the wall lie in the Foreign Intelligence Surveillance Act of 1978, which regulates the government’s ability to conduct electronic surveillance in certain types of national-security investigations.\textsuperscript{56} As originally enacted, FISA required the government to certify to the Foreign Intelligence Surveillance Court that “the purpose” of proposed surveillance was “to obtain foreign intelligence.”\textsuperscript{57} 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.\textsuperscript{58} The concern was with ensuring that the government didn’t use FISA to circumvent Title III (and the Fourth Amendment values it reinforced). Over the years, Congress,\textsuperscript{59} the executive branch,\textsuperscript{60} and federal courts\textsuperscript{61} 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.\textsuperscript{62} 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. 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.

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. In other words, information sharing was a proxy for purpose. The Justice Department therefore segregated its cops and spies to reduce the risk that the FISA court would deem the primary purpose of surveillance to be something other than foreign intelligence gathering.63

In particular, DOJ issued two sets of guidelines in 1995 that 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.”64 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.65 The second set of guidelines applied more broadly to all Justice Department intelligence operations. The guidelines stated categorically that law-enforcement officials “shall not . . . instruct the FBI on the operation, continuation, or expansion of FISA electronic surveillance.”66 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 objectives.”67 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.68 (This second set of guidelines was largely reaffirmed in 2001 by President George W. Bush’s Justice Department.69)

63 See Kris, supra note 1, at 497-99.
64 Gorelick memo at 2.
65 Gorelick memo at 3.
66 Reno memo § (A)(6).
67 Reno memo § (A)(6).
68 Reno memo § (A)(7).
69 See Thompson memo at __ (“The 1995 Procedures remain in effect today.”). The Thompson memo made modest adjustments to the standards. It clarified that the 1995 sharing requirement – the FBI must notify the criminal division when an intelligence investigation turns up “facts or circumstances . . . that reasonably indicate that a significant federal crime has been, is being, or may be committed” – was mandatory and that notification must take place “without delay”; it emphasized that the “reasonable indication” standard “is substantially lower than probable cause”; and it defined “significant federal crime” to include “any federal felony.” Thompson memo at __; see also infra notes 70 to 71 and accompanying text.
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.70 In return, criminal investigators could “give guidance to the FBI aimed at preserving the option of criminal prosecution,” such as “advice on the handling of sensitive human sources.”71 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.72 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.73 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.”74

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 9/11.75 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 communicating that information to consular officials at State or intelligence analysts 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. They also knew, thanks to a tip from an official in Saudi Arabia’s intelligence service, that two Saudi citizens – Nawaf al Hazmi and Khaled al Mihdhar – would participate in the meeting. Mihdhar was traveling from Yemen with a stopover in the United

70 Reno memo § (A)(1); cf. Gorelick memo 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”).

71 Reno memo § (A)(6).

72 See 9/11 COMMISSION REPORT, supra note 2, at 78 (describing OIPR as the gatekeeper for the flow of FISA information to criminal prosecutors”).

73 See 9/11 COMMISSION REPORT, supra note 2, at 78 (“Whether the FBI shared with prosecutors information pertinent to possible criminal investigations was left solely to the judgment of the FBI.”).

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

75 The following account draws heavily from LAWRENCE WRIGHT, THE LOOMING TOWER: AL-QAEDA AND THE ROAD TO 9/11, at 308-15, 328-31, 352-54 (2007), and from 9/11 COMMISSION REPORT, supra note 2, at 156-60; 181-82; 266-72.
Arab Emirates; while he was in Dubai, CIA operatives searched his hotel room. They made a copy of his passport, discovering that the State Department had issued him a multiple-entry visa. 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. “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.”

Back in the States, an FBI agent detailed to the CIA counterterrorism center came across the cable and asked for permission to share it with his colleagues at the bureau. His hosts said no. “This is not a matter for the FBI,” he was told. 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. 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.”

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. 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. (If officials had inspected the passenger manifest, they would have seen that Mihdhar was the same flight.) 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.”

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. (He didn’t because he overslept.) 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. The

---

76 WRIGHT, supra note 75, at 311. 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”).

77 WRIGHT, supra note 75, at 311.

78 WRIGHT, supra note 75, at 311.

79 WRIGHT, supra note 75, at 312.

80 WRIGHT, supra note 75, at 312; 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”).
name rang a bell with an FBI agent who was reviewing the interrogation transcripts. He arranged for a photograph of the person he suspected of orchestrating the Cole bombing to be shown to the cameraman; the cameraman confirmed that the man in the picture was Khallad. “That was the first real link between the Cole bombing and al-Qaeda.”81 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.”82 The agent sent another message a few days later. “Again, the agency had nothing to say.”83

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”84 – CIA had begun to share information with FBI intelligence analysts, though perhaps not to optimal levels. (Intelligence agencies may well have special incentives to share during times of crisis in ways they ordinarily would not.85) In late August, Dina Corsi – an intelligence official at FBI headquarters – emailed a group of intelligence operatives directing them to investigate whether or not Khaled al Mihdhar was still in country. She inadvertently copied Steve Bongardt, an FBI agent who was working the criminal investigation of the Cole bombing. Bongardt immediately called Corsi with a demand for more information about Mihdhar. She refused, and asked him to delete the message he had received. Bongardt then fired off an angry email: “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.’”86

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. 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.87 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.”88 A handful of agencies – the Office of the Director of National Intelligence, as well as the Departments of Commerce,

81 Wright, supra note 75, at 329.
82 Wright, supra note 75, at 329.
83 Wright, supra note 75, at 330.
84 9/11 Commission Report, supra note 2, at 254.
85 See infra note 219.
86 9/11 Commission Report, supra note 2, at 271.
87 See Memorandum for the Heads of Executive Departments and Agencies re: Guidelines and Requirements in Support of the Information Sharing Environment (Dec. 16, 2005) (“ISE Guidelines”). For further discussion, see infra notes 133 to 136 and accompanying text.
88 ISE Guidelines at __.
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.” In other words, agencies may agree to foreign ORCON restrictions. 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”) and Executive Order 13388 (which directs agencies to share terrorism information with one another) “is consistent” with such arrangements. The effect of the Guideline 4 report is to green-light individual agencies that negotiate with foreign counterparts to agree to (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.” CUI is not classified, but the government nevertheless believes the data to be sufficiently sensitive that its public release could harm the national security. 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” and “chemical vulnerability information.” With nearly 60 different CUI categories, 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.” As a result, “[m]ore than half of the agencies reported encountering challenges in sharing such information.” In response, President Bush issued a directive on May 9, 2008 instructing all

---

89 ISE Guidelines § 2(d).
90 Guideline 4 report at 8. 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.
91 See infra notes 118 to 124 and accompanying text.
92 See infra notes 130 to 132 and accompanying text.
93 Guideline 4 report at 10.
94 GAO Report 06-385, at 5.
executive-branch agencies to adopt common CUI rules. 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. The directive also orders agencies to use common handling markings, which indicate the conditions under which recipients of the document must store it. 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. They are: “Protected Critical Infrastructure Information” (data about critical infrastructure, such as railways and internet backbone), “Sensitive Security Information” (information about the screening of airline passengers, baggage, and cargo), “Chemical Vulnerability Information” (information about chemical-plant facilities, processes, and security plans), and “Safeguards Information” (data about at nuclear power plants and materials). The Department of Homeland Security controls each type of information; in most cases, DHS acquires the data when private firms voluntarily turn it over to the agency. 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 attack on the USS Cole. Naturally, they wanted access to NSA intercepts of Osama bin Laden’s satellite telephone calls. Initially the NSA was willing to share the intercepts but later began to withhold them, evidently to protect sensitive intelligence sources and methods. 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.” Eventually the NSA relented and handed over the intercepts.

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

---

95 See Memorandum for the Heads of Executive Departments and Agencies re: Designation and Sharing of Controlled Unclassified Information (CUI) (May 9, 2008).
96 See 6 C.F.R. pt. 29.
98 See 6 C.F.R. § 27.400.
99 See 10 C.F.R. § 73.21.
100 WRIGHT, supra note 75, at 344.
measures do no more than eliminate legal restrictions on information sharing. Others more ambitiously, if not completely successfully, 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. That 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), which generally bars attorneys for the government from “disclos[ing] a matter occurring before the grand jury.” After PATRIOT, 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.” They need not obtain a judge’s approval before doing so. Section 203 made similar changes to the federal wiretap statute, which was read to restrict law-enforcement officers to sharing the fruits of electronic surveillance with other criminal investigators. The PATRIOT Act eliminated that limitation, authorizing cops to share intercepts with spies “to the extent that such contents include foreign intelligence or counterintelligence . . . or foreign intelligence information.” 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.”

---

101 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 http://www.usdoj.gov/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. So the Senate and the House of Representatives picked new names. The Senate bill was dubbed the “Uniting and Strengthening America Act,” while its House counterpart was the even more imaginative “Provide Appropriate Tools Required to Intercept and Obstruct Terrorism.” 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) Act of 2001,” Pub. L. No. 107-56, 115 Stat. 272 (2001). See generally Beryl A. Howell, Seven Weeks: The Making of the USA PATRIOT Act, 72 GEO. WASH. L. REV. 1145, __ (2004)


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

The PATRIOT Act promoted the flow of information in the opposite direction, as well—from intelligence analysts to law-enforcement officers. As discussed above, the Justice Department had erected a “wall” isolating the FBI’s intelligence analysts from officials responsible for investigating ordinary crimes. Sections 218 and 504 sought to abolish 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. Section 504 was even more explicit. It provides that intelligence officials “may consult with Federal law enforcement officers to coordinate efforts” against national-security threats. 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. 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 PATRIOT “accomplished” the goal of “eliminating artificial barriers to the pooling of intelligence data.” Those plaudits are unwarranted. PATRIOT’s information-sharing ambitions are actually quite modest. The act is largely limited to eliminating various statutory and other 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.

The Homeland Security Act of 2002 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. 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

---

107 See supra notes 51 to 73 and accompanying text.
109 USA PATRIOT Act § 504, 115 Stat. at ___ (codified at 50 U.S.C. §§ 1806(k) & 1825(k)).
110 In re Sealed Case, 310 F.3d 717 (FISCR 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 FISCR 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).
111 POSNER, SURPRISE ATTACKS, supra note 1, at 122.
local personnel.” 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 corpus of counterterrorism information; instead, the data is housed at various points throughout the intelligence system.

The Homeland Security Act contains another, lesser-noticed information-sharing provision. Section 202 granted 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.” 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. 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 (“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 – what Judge Posner calls an “inverted-V pattern” arrangement. 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.

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’s exhortations have their limits. While Congress imposed duties

---

113 HSA § 892(b)(1), 116 Stat. at 2253. The President delegated to the Secretary of Homeland Security his responsibility for establishing the procedures contemplated by section 892. See EO 13,311 (July 29, 2003).
114 Homeland Security Act § 202(a)(1), (2).
115 Homeland Security Act § 202(b)(1), (2).
116 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.
117 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 __, but today that role is performed by the National Counterterrorism Center.
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 further evolved in the Intelligence Reform and Terrorism Prevention Act of 2004.\(^{118}\) IRTPA’s boldest – and most controversial\(^{119}\) – move was to reorganize the intelligence community by placing it under the oversight of a new “Director of National Intelligence” (who also would serve as the chief intelligence advisor to the president).\(^{120}\) 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.”\(^{121}\) 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, the Information Sharing Council, and so on – but it offers only the barest guidance on what policies those institutions should pursue.\(^{122}\)

For example, IRTPA calls for the Information Sharing Environment to be “decentralized, distributed, and coordinated.”\(^{123}\) 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), 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). 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 of originator control,” as well as by “providing affirmative incentives for information sharing.”\(^{124}\) Unfortunately, IRTPA doesn’t contribute much more than general platitudes. The legislation reflects only the thinnest analysis of why it might be in agencies’ interest 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-sharing incentives. IRTPA asks the right questions, but it is woefully short on answers.


\(^{119}\) See generally POSNER, SURPRISE ATTACKS, supra note 1 (criticizing creation of Director of National Intelligence).

\(^{120}\) IRTPA § 1001(a).

\(^{121}\) IRTPA § 1016(a)(2).

\(^{122}\) See IRTPA § 1016(b)(1)(C) (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”).

\(^{123}\) IRTPA § 1016(b)(2).

\(^{124}\) IRTPA § 1016(d)(3).
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.”\footnote{EO 13,354 § 1(a) (Aug. 27, 2004).} It further created a National Counterterrorism Center 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.”\footnote{EO 13,354 § 3(a).} 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 terrorist groups.”\footnote{EO 13,354 § 3(a), (d).} For their part, intelligence agencies are to “promptly give access to [terrorism] information to the Director of the Center.”\footnote{EO 13,354 § 6(a)(i)(A).} They also “may query Center data for any information to assist in their respective responsibilities.”\footnote{EO 13,354 § 3(c); see also id. § 3(c) (“The Center shall ensure that agencies have access to and receive intelligence needed to accomplish their assigned activities.”).} 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.”\footnote{EO 13,356 § 2. President Bush later revoked Executive Order 13356, but its substantive provisions live on largely unchanged in a successor directive. See EO 13,388 (Oct. 25, 2005).} Unlike its twin, this order contemplates a distributed network in which information is held by a number of different agencies. Intelligence agencies are to exchange information with one another directly, not route it through a central data broker like the NCTC. 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.”\footnote{EO 13,356 § 3(e).} 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.\footnote{EO 13,356 § 3(a), (c), (d).} 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.\textsuperscript{133} 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. They also take 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.”\textsuperscript{134} 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, by reducing disincentives to such sharing, and by holding their senior managers and officials accountable for improved and increased sharing of such information.\textsuperscript{135}

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.\textsuperscript{136} 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.

III. WHY DON’T INTELLIGENCE AGENCIES SHARE INFORMATION?

The tendency of intelligence agencies to hoard information is a classic problem of agency costs – in particular, the costs principals incur when their agents have interests that diverge from their own. As we saw in Part II, the federal government’s principals (Congress and the president) have, through a series of legislation and directives, instructed their agents (members of the nation’s 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

\textsuperscript{133} For additional discussion of the guidelines, see supra notes87 to 93 and accompanying text.

\textsuperscript{134} ISE Guidelines § 1.

\textsuperscript{135} ISE Guidelines § 3.

\textsuperscript{136} ISE Guidelines § 3(a), (b).
intelligence assessments, which in turn enables principals to make better decisions. But intelligence agencies have an interest in hoarding. This Part explains why. The first subsection considers what intelligence agencies maximize and offers some preliminary observations on how information sharing can undermine those goods. The next three subsections 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. 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 email, 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.

Some caveats are needed. The behavior of public agencies often resembles the behavior of private firms but they are not on all fours. 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

---

137 See POSNER, SURPRISE ATTACKS, supra note 1, at 43 (“[T]he different intelligence services tend, because information is power, to hoard it.”).

138 See generally LOWENTHAL, supra note 24, at 55-67 (summarizing the intelligence-production cycle).

139 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 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 the agency’s superior and as a consumer of their goods – it makes more sense to think of the system as comprising separate, rival firms.

140 See POSNER, SURPRISE ATTACKS, supra note 1, at 105; JAMES Q. WILSON, BUREAUCRACY __ (2000).
outlays, 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. (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 outputs over a period of time. 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.

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.” 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.

---


142 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.

143 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. 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 their 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 assessments, but they also reflect unrelated factors such as the extent of their cooperation with Congress and the influence of their congressional patrons.

144 Posner, Surprise Attacks, supra note 1, at 105; see also Lowenthal, supra note 24, at 216.
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. But it appears that intelligence agencies in particular seek 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. 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. The 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, a digest of intelligence analyses that the Director of National Intelligence provides to the president every morning. It is considered a crowning achievement within the intelligence community for an analyst to have one of his reports included in the PDB. (This creates incentives that distort intelligence analysis. The items that make it into the PDB are the ones with the gripping headline summaries. Analysts thus will tend to overstate conclusions that are in fact tentative,

---

145 See, e.g., NISKANEN, supra note 141, 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 the ease of managing the bureau”).

146 Notice that budgets aren’t on the list. Contra NISKANEN, supra note 141, at 38-39; William A. Niskanen, Jr., Bureaucrats and Politicians, 18 J. L. & ECON. 617, __ (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 they do (i.e., when doing so would enhance an agency’s ability to achieve its priorities). But sometimes agencies 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 153 to 157 and accompanying text. In other words, what looks like budget maximization in reality is often autonomy maximization. Cf. WILSON, supra note 140, at x (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”).
and resist caveating their conclusions by pointing to contrary evidence. 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.

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. 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. 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.

How does information sharing threaten an agency’s ability to influence the decisions of senior executive-branch officials? It’s basically a free-rider problem. 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. 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) 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

---

147 See WMD REPORT, supra note 2, at 14, 181-82.
148 See LOWENTHAL, supra note 24, at 187; POSNER, SURPRISE ATTACKS, supra note 1, at 115.
149 See, e.g., POSNER, UNCERTAIN SHIELD, supra note 7, at 34; WMD REPORT, supra note 2, at 189-92.
150 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”).
151 See POSNER, COUNTERING TERRORISM, supra note 33, at 84; POSNER, SURPRISE ATTACKS, supra note 1, at 113. 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 150, at 234.
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 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. 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, while 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 FBI’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.152 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).153 This is not to say agencies invariably engage in what Professor Todd Zywicki calls “empire building.”154 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

---

152 See infra Part III.D.

153 See WILSON, supra note 140, at 182 (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”).

FDCA, thereby furthering its core mission of promoting public health. But sometimes autonomy maximization takes the form of disclaimers of power. For many years, the Army Corps of Engineers declined to extend environmental protections to wetlands, notwithstanding fairly clear signals that Congress wanted it to do so. 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. Likewise, the FBI for years resisted congressional calls to assume responsibility for narcotics investigations. 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.

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. One of the most pronounced fault lines is between the FBI and CIA, both of which have wanted to take the lead in domestic counterespionage operations. 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 classic counterespionage technique). 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.

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 – the predecessor of the CIA – mounted a black-bag job at the Spanish embassy in Washington, DC. The spies were to retrieve and copy a cipher tape from an embassy safe, so as

157 WILSON, supra note 140, at 182-95; Sales & Adler.
158 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”).
160 See Banks, supra note 3, at 1152; LOWENTHAL, supra note 24, at 157-58.
to better eavesdrop on Axis communications. 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. They arrived at the embassy in a squad car, with lights and sirens blaring—risking the CIA operatives’ cover and bringing the operation to a noisy end.161 “On the eve of landings in North Africa, . . . Hoover’s men had come dangerously close to exposing key Allied cipher operations.”162

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 their interests, giving them an opportunity to muscle in and take control. 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 intellectual-property 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.163 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.”164 This right to exclude derives from classification standards and other information-access rules.165 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 marked with the even more rarefied classification “Top Secret/Secure Compartmented Information,” still more

161 See RIEBLING, supra note 159, at 40-42.
162 RIEBLING, supra note 159, at 41.
163 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”).
165 See LOWENTHAL, supra note 24, at 76, 153-54; POSNER, COUNTERING TERRORISM, supra note 33, at 85.
potential users are excluded. (For some of 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” – i.e., those who don’t require the data to do their jobs properly.

Indeed, 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.”166 Another law makes it a crime to give “an unauthorized person” information about “the communication intelligence activities of the United States.”167 The meaning and scope – and constitutionality – of the Espionage Act in particular are notoriously uncertain,168 but the general thrust of these laws is fairly straightforward: Agencies have an obligation, enforceable by criminal sanctions, to keep classified information out of unauthorized hands.

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. The number of such exchanges is probably suboptimally low, and the absence of price information makes it difficult to ascertain the value of a given piece of data to either the originating agency or the recipient. But despite the relative dearth of such exchanges and their relatively high transaction costs, intelligence agencies retain the right to alienate information in a variety of ways.

If intelligence agencies have a quasi-property interest in the national-security data they possess, then to what IP species does it belong? The most obvious candidate is trade secrets.169

166 18 U.S.C. § 793(d).
169 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 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.,
A trade secret is business information that derives value from the fact that it is not generally known, and that its owner strives to keep secret. By definition a trade secret has not been placed in the public domain. 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. 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.)

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. Sometimes the confidentiality obligations are explicit contractual terms; sometimes courts imply them. 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 on the condition that the recipient not further share the data. This is known as originator controls, or ORCON. For instance, an interagency memorandum of understanding might call for DHS to share its threat assessments of U.S.-bound

---

JEM 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.

170 See Uniform Trade Secrets Act § 1(4); see also RESTATEMENT OF TORTS § 757 cmt. b.


172 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)).

173 See Uniform Trade Secrets Act § 1(2) (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.

174 See LOWENTHAL, supra note 24, at 154.
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. FBI intelligence officials kept information behind the wall 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 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 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 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. 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.

175 See supra Part II.A.1.
176 See supra notes 94 to 99 and accompanying text.
C. . . as an Antitrust Problem

Antitrust law offers a second lens to examine intelligence agencies’ reluctance to share information.177 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.178 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.179 The intelligence oligopoly is insulated against competition by massive entry barriers.180 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 dominant – 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.181 For example, the National Security Agency’s worldwide network of electronic eavesdropping equipment gives it a unique ability to collect phone calls and emails overseas, which in turn yields a dominant NSA position in the submarket for SIGINT-based intelligence assessments. Similarly, the National Geospatial-Intelligence Agency’s fleet of satellites gives it a unique ability to collect overhead

177 Antitrust law frequently grapples with information-sharing problems. See generally Aviram & Tor, supra note 150. 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, 473-74 (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 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 IV.B.


179 See HOVENKAMP, supra note 178, § 1.5c.

180 See HOVENKAMP, supra note 178, § 12.4b5 (“[G]overnment regulation, licensing and entry restrictions collectively create among the greatest and most effective entry barriers.”).

181 See HOVENKAMP, supra note 178, § 9.1.
imagery, 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.\(^\text{182}\) Microsoft threatened to cancel the Apple version of its popular Office software to strengthen its hand in the market for internet browsers.\(^\text{183}\) Intelligence 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.\(^\text{184}\) 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.\(^\text{185}\) 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.\(^\text{186}\) 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.\(^\text{187}\) 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.

\(^{182}\) See HOVENKAMP, supra note 178, § 7.5; see also United States v. Colgate & Co., 250 U.S. 300, 307 (1919) (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”).

\(^{183}\) United States v. Microsoft Corp., 253 F.3d 34, 72-74 (D.C. Cir. 2001).

\(^{184}\) See supra Part II.A.2.

\(^{185}\) See WRIGHT, supra note 75, at __ (discussing CIA hostility toward lead FBI counterterrorism investigator).

\(^{186}\) See POSNER, SURPRISE ATTACKS, supra note 1, at 27 (discussing difficulty of infiltrating Islamist terrorist groups).

\(^{187}\) See supra note 100 and accompanying text.
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. 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. 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 exemption amounts to an exclusive deal. 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, 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. 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. Price fixing isn’t possible in the intelligence market, because the compensation agencies receive for their products is set by the president. 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, intelligence agencies’ oligopoly powers are offset by the monopsony power of the sole intelligence consumer—the presidency. The upward price pressure that 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 cartel. Such an arrangement would give each agency (or allow an agency to maintain) a formal position

\[188\] See supra notes 94 to 99 and accompanying text.

\[189\] See HOVENKAMP, supra note 178, § 10.8e.

\[190\] See HOVENKAMP, supra note 178, § 4.1; see also United States v. Socony-Vacuum Oil Co., Inc., 310 U.S. 150, __ (1940) (holding that price-fixing agreements are per se illegal under the Sherman Act).

\[191\] See HOVENKAMP, supra note 178, § 5.2b4; see also United States v. Topco Assocs., Inc., 405 U.S. 596, __ (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 non-price competition may occur. A market division amounts to an agreement among firms not to compete on any terms, at least within the relevant market.
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. 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. Its stated objective is to facilitate the sharing of information obtained from foreign governments. Yet it contains an exception that devours the rule: It accepts foreign ORCON restrictions. Thus when the FBI enters an agreement with 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 from its British counterpart 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 include such restrictions in information sharing agreements.”

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 their relationships with their overseas counterparts; 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. 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

---

192 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.”).

193 See supra notes 87 to 93 and accompanying text.

194 Guideline 4 report at 9.

195 See LOWENTHAL, supra note 24, at 99 (intelligence agencies strive to maintain foreign liaison relationships).

196 See generally George J. Stigler, A Theory of Oligopoly, 72 J. POL. ECON. 44 (1964); see also HOVENKAMP, supra note 178, § 4.1.
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,\textsuperscript{197} and when the FBI detected the planned black-bag job at the Spanish embassy\textsuperscript{198}).

\textit{D. \ldots as an Organizational-Theory Problem}

Organizational theory offers a third lens through which intelligence agencies’ tendency to hoard might be understood.\textsuperscript{199} Information sharing can be risky, and intelligence officials are conditioned by their agencies’ respective institutional cultures to avoid risks.\textsuperscript{200} 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. 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.\textsuperscript{201} 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 institutional cultures. “Culture is to the organization what personality is to the individual – a hidden yet unifying theme that provides meaning, direction, and mobilization.”\textsuperscript{202} 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. In a nutshell, organization behavior is the sum of individual employee behavior, and individual employee 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.\textsuperscript{203} That cultural trait is not an accident; it is the product of specific incentive structures within

\textsuperscript{197} See supra note 100 and accompanying text.

\textsuperscript{198} See supra notes 161 to 162 and accompanying text.


\textsuperscript{200} See Banks, supra note 3, at 1172; Lerner, supra note 1, at 505.

\textsuperscript{201} 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 or CIA’s surveillance of domestic antiwar activists.


\textsuperscript{203} Some scholars believe that government employees as a group are systematically more risk averse than their private-sector counterparts. Evidence of this aversion is that government employees are willing to forego the chance of higher salaries in the private sector in exchange for greater protections against performance-related firings. See,
intelligence agencies. Intelligence 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. The expected costs of boldness exceed the expected benefits, and that asymmetry naturally inclines the official to avoid risks. Notice that I am using the expression “risk averse” in a colloquial 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.\(^{204}\)

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.”\(^{205}\)) Which option would a rational analyst pick?

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.\(^{206}\) 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


\(^{205}\) Posner, Uncertain Shield, supra note 7, at 62.

\(^{206}\) 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 fired.
propounding an unorthodox (and ultimately accurate) opinion is considerable. These possibilities can be illustrated in a basic matrix:

<table>
<thead>
<tr>
<th>Consensus</th>
<th>Correct</th>
<th>Incorrect</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(1) Credit diffused; low per capita benefit</td>
<td>(2) Blame diffused; low per capita cost</td>
</tr>
<tr>
<td>Unorthodox</td>
<td>(3) Full credit; high per capita benefit</td>
<td>(4) Full blame; high per capita cost</td>
</tr>
</tbody>
</table>

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 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. 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 zebras in Siberia. 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.

---

207 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 84 to 86 and accompanying text, does not appear to have been rewarded for his prescience.

208 See ALEKSANDR SOLZHENITSYN, ONE DAY IN THE LIFE OF IVAN DENISOVICH (___).

209 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
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; in the 1990s, FBI intelligence officials were told it was a “career stopper” to share information. 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. Some are even buying insurance to cover their legal expenses in the event they face criminal charges. 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 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.” An official who flouts the act faces a year in jail, a criminal fine, and loss of government employment. The problem is that the category of persons “authorized by law” to see the data operations like paramilitary activities. These officials likely derive significant psychic income from their jobs – e.g., feelings of exhilaration from participating in a successful strike on an al Qaeda training camp – and the psychic income is probably 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).

---

210 See Kris, supra note 1, at 501; see also 9/11 COMMISSION REPORT, supra note 2, at 79.
211 See BENJAMIN WITTES, LAW AND THE LONG WAR 188 (2008) (“We are, in short, asking men and women in the service of their country to live their professional lives standing on and leaning over the boarder of criminal conduct we lack the courage to define precisely.”).
212 See GOLDSMITH, supra note 204, at 95-96
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. 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,” 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.) 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 violations, the greater the costs. 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. 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

216 5 U.S.C. § 552a(b)(3).
217 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.
assassinations, interfering in foreign elections, and so on. 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.\textsuperscript{218} The point is not to suggest 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.\textsuperscript{219}

The wall is an instance of cultural risk aversion resulting in hoarding.\textsuperscript{220} The Justice Department didn’t build the wall between cops and spies because it was thought to be legally necessary.\textsuperscript{221} To the contrary, the agency was quite clear that its sharing restrictions “go beyond what is legally required.”\textsuperscript{222} What DOJ feared was legal uncertainty: How would the FISA court apply the primary-purpose standard? It also worried that appearance problems – namely, the appearance 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. 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.\textsuperscript{223}

\textsuperscript{218} See, e.g., COLL, \textit{supra} note 102, at 43-44.

\textsuperscript{219} These incentives may be reversed in times of crisis. Professor Jack Goldsmith – onetime 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, \textit{supra} note 204, 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). 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 \textit{infra} note 223 – 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 \textit{supra} notes 84 to 86 and accompanying text.

\textsuperscript{220} See \textit{supra} Part II.A.1.

\textsuperscript{221} See Banks, \textit{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”). \textit{Contra} 9/11 COMMISSION REPORT, \textit{supra} note 2, at 79; POSNER, \textit{SURPRISE ATTACKS}, \textit{supra} note 1, at 31-32.

\textsuperscript{222} Gorelick memo at 2.

\textsuperscript{223} 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 DNI 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, \textit{COUNTERING TERRORISM}, \textit{supra} note 33, at 44. Why, then, don’t the fears of autonomy loss 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.
IV. WHAT CAN BE DONE?

Parts II and III 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.\footnote{Cf. Banks, supra note 3, at 1193 (“It may make 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.”).} 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 agency information sharing.

This is a good place for modesty. I am more confident in the diagnosis than in the cures that might be prescribed, and some of the possibilities are more feasible than others. What follows in this Part should not be understood as an endorsement of any particular remedy to the hoarding problem. My objective is to lay out a menu of possible options from which reformers may wish to pick. Another important caveat: I am not arguing 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.\footnote{Cf. Swire, supra note 1, at 952 (proposing a “due diligence checklist” for determining when sharing should and should not take place).} The solution to the hoarding problem is not to compel data exchange in all cases, but rather to establish mechanisms capable of sorting the restrictions that are justified from the ones that are not.\footnote{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.” Testimony of Lee H. Hamilton Before the Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment, Comm. on Homeland Security, U.S. House of Representatives, Nov. 8, 2005; 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 be contrast, the costs of sharing (transfer or termination, criminal sanctions, etc.) are borne directly by the agency officials who authorized it.}

A. Intellectual-Property Solutions

One solution that can be dismissed out of hand is to abolish intelligence agencies’ property interests in information altogether.\footnote{Cf. Banks, supra note 3, at 1193 (“It may make 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.”).} Doing so would destroy agencies’ incentives to
gather information in the first place; it would result in significant commons problems. 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 – 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.

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 would also 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). A proposal for broad IP protections might appear counterintuitive.

Therefore be an explicit statement of policy that originators or producers do not own or control the information they produce.

---

228 See generally Harold Demsetz, Toward a Theory of Property Rights, 57 AM. ECON. REV. 347 (1967).
229 Cf. Posner, Uncertain Shield, supra note 7, at 17 (arguing that recognition of property interests in intelligence information “might be needed to impart adequate incentives to intelligence agencies to obtain good data and produce cogent analysis”).
230 Finished intelligence assessments may be thought of, in copyright terms, as original works that “possess at least some minimal degree of creativity.” Feist Publications, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, ___ (1991); see also __ NIMMER ON COPYRIGHT § 2.01[B]. The creative element here consists of intelligence analysts assembling, synthesizing, and interpreting raw information, thereby yielding an entirely new work. The assessments also could
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 (the PTO almost always publishes the application, thereby eliminating any trade secret protections). 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 extent 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 and, as it was originally 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 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 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 __. 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 (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. National Basketball Ass’n v. Motorola, Inc., 105 F.3d 841, __ (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 Directive 96/9/EC (Mar. 11, 1996). 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). Whatever the appropriate IP analogies, the basic point is simple: Finished assessments and raw data both should be protected under a hybrid system.

231 See supra notes 125 to 129 and accompanying text.
conceived, the Department of Homeland Security. 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.”) 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. 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.

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. 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

---

233 See supra notes 114 to 117 and accompanying text.


235 See FOURTH MARKLE REPORT, supra note 2, at 11-14.

236 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 33, at 84. Publication of capsule summaries in a searchable index probably poses fewer risks.

237 2 NIMMER ON COPYRIGHT § 8.23[A][1].
efforts of an originator; it should not be allowed “to reap where it has not sown.”238 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 for more utilitarian aims.239 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. (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.240 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.)

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.241 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 made 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.

240 4 NIMMER ON COPYRIGHT § 13.05.
Yet an originating agency is unlikely to regard a footnote as adequate compensation to offset its loss of relative influence and autonomy. 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 radical 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. 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 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, 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. 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.

242 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).

Besides, how do you monetize influence and autonomy?\textsuperscript{244} 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.\textsuperscript{245} While this reform is concededly radical, it might be worth considering if only because it casts in sharp relief the problems of data exchange and compensation and because it may spur other solutions.

\textbf{B. Antitrust Solutions}

The intelligence system needs a robust enforcement mechanism to promote information sharing and resolve sharing conflicts. In the absence of such a scheme, an agency whose rival refuses to share has only one remedy: It can retaliate by withholding its own information. Hoarding is met by more hoarding, and the flow of data is gradually choked off. An enforcement scheme would enable interagency conflicts to be resolved outright, rather than morph into tit-for-tat brinkmanship. Federal antitrust law uses a suite of tools to prevent anticompetitive conduct and promote consumer welfare – centralized regulation and enforcement by administrative agencies, private enforcement through civil lawsuits for money damages, and private ordering that harnesses market forces. Reformers 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 of the Information Sharing Environment, whose office was established in 2004, is broadly assigned “responsibilit[y] for information sharing across the Federal Government.”\textsuperscript{246} 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.\textsuperscript{247} But only a rough counterpart: His powers are weak to the point of nonexistence. While the PM in theory has authority to establish federal information-sharing policy,\textsuperscript{248} 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.\textsuperscript{249} 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

\textsuperscript{244} Cf. Posner, Uncertain Shield, supra note 7, at 148 (“A government agency does not produce a monetized or readily monetizable output.”).


\textsuperscript{246} IRTPA § 1016(f)(1).

\textsuperscript{247} See Hovenkamp, supra note 178, § 15.1.

\textsuperscript{248} IRTPA § 1016(f)(2)(A)(ii).

\textsuperscript{249} See Hovenkamp, supra note 178, §§ 15.1a, 15.1b.
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.250)
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 intelligence 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 preceded by elaborate administrative – and maybe
judicial – procedures. 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 far from clear that the president
has authority under the Constitution unilaterally to impound or reprogram appropriated funds, 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.251 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. There’s a catch:
Only the first firm to come forward is assured of immunity. The effect is to create a strong
incentive to be the first mover; 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 go down.

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

250 See supra notes 114 to 117 and accompanying text.
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.\textsuperscript{252} 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.\textsuperscript{253} 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.\textsuperscript{254} 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 unnoticed if the system relied only on a central regulator.\textsuperscript{255} (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,\textsuperscript{256} but it has used such

\textsuperscript{252} Cf. Posner, Surprise Attacks, supra note 1, at 42 (arguing that “an intelligence 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”).

\textsuperscript{253} See Hovenkamp, supra note 178, § 16.2.

\textsuperscript{254} Cf. Hayek, supra note 243, at __.

\textsuperscript{255} 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.

\textsuperscript{256} See, e.g., APA § 554(d) (providing that “an 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”).
an approach in other contexts. Before the old Immigration and Naturalization Service was split in two and transferred from the Justice Department to Homeland Security, the Attorney General was both prosecutor and judge. He was responsible for deciding whether to file charges before DOJ’s immigration judges, and also had responsibility for reviewing (and ultimately rejecting) the immigration judges’ decisions. 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.257

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.258

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 heavily on private ordering to produce greater levels of information sharing. Indeed, the current system basically leaves agencies to their own devices, and look where it’s

257 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 ongoing investigation with the Secret Service). 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.

258 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 148 to 149 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.
gotten us. 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 that signal enables 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 market 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 signals could be overcome if intelligence agencies were allowed to buy and sell information, 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. 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. 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 were nowhere near as accurate. (Perhaps one reason for the effectiveness of private intelligence is that private-sector employers have greater ability to offer tangible rewards, like cash bounties, to high-performing employees than government employers do.) Even more important, private firms would inject a measure of competition into the intelligence market. Incumbent intelligence agencies would find themselves competing for policymakers’ attention with new entrants. 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

259 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).

260 See generally POSNER, COUNTERING TERRORISM, supra note 33, at 72-81.

261 See COLL, supra note 102, at 159-60; DANIEL PATRICK MOYNIHAN, SECRECY: THE AMERICAN EXPERIENCE __ (1999).
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 that takes place, 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 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 president 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. What’s needed are new mechanisms that can counter intelligence analysts’ natural (and rational) risk aversion and create new incentives to engage in sharing that is desirable but risky. 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. (This proposal is more radical in that the PM would be exercising fairly fine-grained oversight over intelligence agencies’ day-to-day personnel decisions.) 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, which 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, whether successful or not. 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 have two ways to reduce the expected costs of information sharing – they could either reduce the magnitude of the harms that sharing threatens to produce, or they could reduce 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. Congress should consider amending the remaining statutes that continue to interpose legal barriers to effective information sharing. Delving into the details of that project would take us well beyond the scope of this article; I plan to address the problem in a future work. For now, we can offer a few preliminary observations on how to reduce both the legal sanctions applicable to intelligence officials who share, as well as the likelihood that those sanctions will be imposed.

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 intelligence 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.
Even 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. The basic idea is reliance. 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. 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, 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.262

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 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.263 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

262 See GOLDSMITH, supra note 204, at 96-97 (discussing OLC’s power “to dispense get-out-of-jail-free cards”).

263 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”).
he therefore will 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.” 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.

Another option would be to adopt policies aimed at weakening individual employees’ cultural commitments to their particular agencies and strengthening their loyalties to the intelligence community as a whole. The DNI already has begun to require that officials serve a tour of duty at another intelligence agency to be promoted to the senior ranks. (This reform appears to have been inspired by the Goldwater-Nichols Act of 1986, which sought to minimize rivalries among the various armed forces in part by requiring officers to serve at least one joint duty assignment as a precondition of promotion to flag rank.) Other measures could include community-wide recruitment and training programs (which not only would foster relationships among rookie analysts destined for different agencies, but also would help build a common culture across the entire community) and more extensive personnel exchanges among intelligence agencies. These sorts of measures might encourage officials to share information by weakening (even if not eliminating) their perception of other intelligence agencies as hostile competitors.

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 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 mustn’t 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 crop up 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

264 ISE Guidelines § 3(a), (b).
265 See FOURTH MARKLE REPORT, supra note 2, at 18.
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 are just as promising. 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 information sharing.