

Mending Walls: Information Sharing After the USA PATRIOT Act

Nathan Alexander Sales*

*Something there is that doesn't love a wall,
That sends the frozen-ground-swell under it,
And spills the upper boulders in the sun;
And makes gaps even two can pass abreast.*
—Robert Frost, “Mending Wall”

Introduction.....	1796
I. Two Cheers for Information Sharing.....	1799
II. Walls: Past and Present.....	1807
A. The Life and Times of the FISA Wall	1809
B. National Security Act of 1947	1813
C. Posse Comitatus Act	1819
D. Privacy Act.....	1830
III. Recalibrating the Law and Policy of Information Sharing	1836
A. Pretext Concerns	1837
B. Firewall Concerns	1840
C. Republicanism Concerns	1844
D. Privacy Concerns	1847

* Assistant Professor of Law, George Mason University School of Law. I’m grateful to Bill Banks, Nate Cash, Bobby Chesney, Craig Lerner, Greg McNeal, Hugo Teufel, and Todd Zywicki for helpful comments on earlier versions of this Article. Special thanks to the Center for Infrastructure Protection and Homeland Security for generous financial support. I worked on a number of information-sharing initiatives while serving at the U.S. Departments of Justice and Homeland Security, but the opinions expressed in this Article are solely mine.

Conclusion	1853
------------------	------

Introduction

The conventional wisdom is that the USA PATRIOT Act tore down the wall.¹ The conventional wisdom is mistaken.

It was the summer of 2001, and FBI agents were frantically trying to locate a suspected al Qaeda operative named Khalid al-Mihdhar. Toward the end of August, Steve Bongardt, who was working the criminal investigation of the USS *Cole* bombing, received an e-mail from one of the Bureau's intelligence officials; it mentioned that al-Mihdhar might have entered the United States. His curiosity piqued, Bongardt picked up the phone and asked his colleague to tell him more. What he got was an order to delete the message; it was sent to him by accident. Bongardt then fired off an angry e-mail: "Whatever has happened to this—someday somebody will die—and wall or not—the public will not understand why we were not more effective and throwing every resource we had at certain 'problems.'"²

He was right. A few weeks later Khalid al-Mihdhar helped hijack American Airlines Flight 77 and crash it into the Pentagon.

After 9/11, it was widely agreed that national security officials needed to do a better job sharing information with one another.³ The free flow of data, it was argued, would help them "connect[] the dots" and prevent future attacks.⁴ An early example of this consensus was the USA PATRIOT Act,⁵ which amended a provision in the Foreign Intelligence Surveillance Act (FISA) that prevented intelligence officials at the FBI from exchanging data

1. See, e.g., RICHARD A. POSNER, PREVENTING SURPRISE ATTACKS 122 (2005) (arguing that the PATRIOT Act "accomplished" the goal of "eliminating artificial barriers to the pooling of intelligence data"); Fred F. Manget, *Intelligence and the Criminal Law System*, 17 STAN. L. & POL'Y REV. 415, 420 (2006) ("The wall is gone.").

2. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 271 (2004) [hereinafter 9/11 COMMISSION REPORT]; LAWRENCE WRIGHT, THE LOOMING TOWER: AL-QAEDA AND THE ROAD TO 9/11, at 353–54 (2006).

3. See 9/11 COMMISSION REPORT, *supra* note 2, at 416–19 (discussing the need for improved information sharing in the Intelligence Community); POSNER, *supra* note 1, at 26, 28 (urging improved cooperation between private and public agencies); Michael V. Hayden, *Balancing Security and Liberty: The Challenge of Sharing Foreign Signals Intelligence*, 19 NOTRE DAME J.L. ETHICS & PUB. POL'Y 247, 257–60 (2005) (calling for expanded information sharing); David S. Kris, *The Rise and Fall of the FISA Wall*, 17 STAN. L. & POL'Y REV. 487, 518, 521–22 (2006) (analyzing the benefits of abolishing the FISA wall); Craig S. Lerner, *The USA PATRIOT Act: Promoting the Cooperation of Foreign Intelligence Gathering and Law Enforcement*, 11 GEO. MASON L. REV. 493, 524–26 (2003) (discussing some benefits of information sharing); Peter P. Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 VILL. L. REV. 951, 951–59 (2006) (discussing which information should be shared and when).

4. 9/11 COMMISSION REPORT, *supra* note 2, at 416.

5. USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered titles of U.S.C.).

with criminal investigators.⁶ Yet even in PATRIOT's wake, a number of walls remain on the statute books.⁷ These legal constraints have attracted virtually no attention, either in academic circles or elsewhere. "[A]ny suggestion that there is still a 'wall' is not considered politically correct."⁸ The issue may have escaped notice, but that does not make it unimportant. The remaining restrictions on information sharing have the potential to affect the full range of agencies with national security responsibilities, from the Intelligence Community to the Armed Forces to law enforcement. They also potentially cover the entire spectrum of data that could be relevant to counterterrorism operations, from electronic-surveillance intercepts to satellite imagery to industrial-facility vulnerability assessments.

This Article attempts to fill that gap in the literature. It has three goals: to weigh the advantages and disadvantages of information sharing; to identify some of the remaining legal restrictions on data exchange, as well as their policy justifications; and to consider whether these laws' underlying values can coexist with expanded sharing.

Part I discusses some of the benefits and costs of data exchange. A principal advantage of sharing is that it enables intelligence agencies to better detect national security threats. By assembling individual tiles that by themselves reveal little, information sharing allows analysts to see the entire mosaic of enemy intentions. Sharing also allows agencies to specialize in the collection of various different types of information; these market niches produce efficiency gains that result in better intelligence product. Yet sharing has its downsides. Data exchange can compromise sensitive intelligence sources and methods by increasing the likelihood that they will leak. It can flood intelligence analysts with troves of data, making it harder to distinguish signal from noise and reinforcing preconceptions about hostile powers' capabilities and intentions. And sharing can burden the privacy interests of persons to whom the data pertains.

Part II analyzes statutory restrictions on information sharing and their policy justifications. It begins with the prototypical wall—FISA's "primary purpose" requirement, which crippled information sharing from the mid-1990s up to the 9/11 attacks. The wall sought to prevent "pretext." It was feared that law enforcement officials might ask intelligence officials to collect evidence for use in criminal proceedings; FISA kept cops from evading the legal limits on domestic surveillance by commissioning spies to do the dirty work for them.

I then turn to some of the remaining statutory restrictions on information sharing. The National Security Act of 1947 bars the CIA from

6. *See id.* § 218 (codified at 50 U.S.C. § 1804(a)(6)(B) (2006)) (permitting the use of FISA when a "significant purpose of the surveillance is to obtain foreign intelligence information").

7. *See infra* Part II.

8. Grant T. Harris, Note, *The CIA Mandate and the War on Terror*, 23 YALE L. & POL'Y REV. 529, 554 (2005).

exercising “police, subpoena, or law enforcement powers” or engaging in “internal security functions.”⁹ Similar to the FISA wall, the 1947 Act thus prevents spies from engaging in pretextual surveillance at the behest of cops. It also reflects “firewall” concerns—the notion that, while it might be appropriate to use unsavory intelligence techniques in the foreign sphere, the government should not operate the same way domestically. The Act’s strictures could prevent the CIA from swapping information with federal law enforcement officials, most notably the FBI. A second restriction is found in the Posse Comitatus Act,¹⁰ which makes it a crime to “use[] any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws.”¹¹ Posse Comitatus is another firewall statute; it insulates domestic law enforcement from the more violent practices that characterize military operations. The Act also reflects “republicanism” concerns—the idea that the Armed Forces must always be subordinate to civilian authorities. The sweeping Posse Comitatus rule may prevent the Armed Forces from sharing information with domestic authorities in the aftermath of a terrorist attack or natural disaster by, for example, providing the FBI with intelligence about the attack site or offering tactical advice on how to manage the disaster zone. The Privacy Act of 1974 offers a third example. It promotes “individual privacy” in two senses: freedom from government observation and the ability to control how information about oneself is presented to the outside world. A restrictive reading of the Act—in particular, the requirement that routine disclosures of covered records must be “compatible with the purpose for which [they were] collected”¹²—could prevent, for example, U.S. Customs and Border Protection (Customs) from sharing data about arriving container ships with National Security Agency (NSA) officials who want to exploit it to screen for terrorist stowaways. In short, the 1947 Act, Posse Comitatus, and the Privacy Act are overbroad. Congress had good reasons to enact these statutes, but they sweep so broadly that they imperil desirable information sharing that does not threaten the harms about which Congress justifiably was concerned.

Part III considers whether it is possible to promote data exchange while remaining faithful to these laws’ underlying pretext, firewall, republicanism, and privacy concerns. The answer, I argue, is yes. My analysis is informed by rational-choice theories of bureaucratic action and focuses on individual and institutional incentives within military and intelligence agencies. It is unlikely that information sharing between the FBI and the CIA under the 1947 Act will raise meaningful pretext problems. The CIA will have strong incentives to decline requests by its bureaucratic rival to collect evidence for use in criminal proceedings because doing so would harm the CIA’s own

9. 50 U.S.C. § 403-4a(d)(1) (2006).

10. 18 U.S.C. § 1385 (2006).

11. *Id.*

12. 5 U.S.C. § 552a(a)(7) (2006).

interests. Similarly, sharing probably won't raise firewall concerns. Data exchange can actually promote firewall principles by mitigating agencies' incentives to mount aggressive operations in inappropriate spheres. Republicanism concerns do not justify sharing restrictions; the potential harms are both slight and unlikely to materialize. And information sharing can preserve privacy values even more effectively than a strict prohibition on data exchange by reducing agencies' incentives to engage in privacy-eroding surveillance.

A few preliminary observations are needed. First, this Article suffers from the same shortcomings that plague virtually all efforts to write about highly classified national security matters—a dearth of publicly available information. A good deal of data about how these statutory barriers affect information sharing among military, intelligence, and law enforcement players presumably remains hidden from public view. In its absence, the most we can hope to do is offer conjectures or educated guesses. Second, eliminating the statutory barriers discussed in this Article will not, without more, lead to the free flow of information. Agencies aren't exactly clamoring to share with one another; as I've argued elsewhere, officials have strong incentives to hoard data, and information sharing will be stymied unless these incentives are recalibrated.¹³ Still, modifying legal rules to permit more sharing is an important first step. Statutory restrictions on data exchange reinforce agencies' worst instincts, ensuring that even less information changes hands.

Two Cheers for Information Sharing

The post-9/11 consensus is that information sharing is a good thing. There is “near universal agreement” that “fighting terror will require deeper coordination than existed heretofore between law enforcement agencies, the CIA, and the military.”¹⁴ Data exchange is worthwhile because it enables officials to piece together the intelligence mosaic, an especially important task in conflicts with nontraditional adversaries such as terrorist organizations.¹⁵ Also, sharing produces efficiency gains by allowing different intelligence agencies to specialize in collecting particular kinds of information.¹⁶ So why only two cheers? Because sometimes data exchange can harm the government's national security interests, to say nothing of the privacy interests of the people to whom the information pertains.

13. See Nathan Alexander Sales, *Share and Share Alike: Intelligence Agencies and Information Sharing*, 78 GEO. WASH. L. REV. 279, 303–13 (2010) (arguing that intelligence agencies hoard to protect their influence and autonomy).

14. Noah Feldman, *Choices of Law, Choices of War*, 25 HARV. J.L. & PUB. POL'Y 457, 482 (2002); see also *supra* note 3.

15. See David E. Pozen, Note, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628, 630–31, 645–46, 651 (2005) (discussing the mosaic theory and its increased prominence after 9/11).

16. Hayden, *supra* note 3, at 258.

The principal advantage of information sharing is that it enables intelligence analysts to better detect threats against the United States. Taken individually, a piece of information might not reveal anything about an adversary's intentions or capabilities.¹⁷ But seemingly innocuous data can become more meaningful, and more sinister, when aggregated with other information.¹⁸ This is known as the mosaic theory.¹⁹ “[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.”²⁰ One tile may not suggest much at all, but the larger mosaic might. The mosaic theory traditionally has been offered as a reason why the government might resist the release of a particular piece of information, as in response to a FOIA request.²¹ Yet it is as much a theory of intelligence analysis as it is a theory of nondisclosure. As long ago as the Revolutionary War, General George Washington—“America’s first spymaster”²²—recognized the importance of collecting and aggregating apparently unrelated pieces of information. “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.”²³

A related benefit is that information sharing can reduce the likelihood of catastrophic intelligence failures.²⁴ “[T]he intelligence failures that hurt the worst have not been those of collection but rather those of dissemination.”²⁵ Some scholars believe that breakdowns in information sharing contributed to

17. Pozen, *supra* note 15, at 630.

18. *Id.*

19. *Id.*

20. J. Roderick MacArthur Found. v. FBI, 102 F.3d 600, 604 (D.C. Cir. 1996) (citation omitted) (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) (explaining that “[t]he significance of one item of information may frequently depend upon knowledge of many other items of information”).

21. *See, e.g.*, *CIA v. Sims*, 471 U.S. 159, 178 (1985) (upholding the CIA’s refusal to divulge identities of private researchers participating in the Agency’s MKULTRA program, 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’” (quoting *Halperin v. CIA*, 629 F.2d 144, 150 (D.C. Cir. 1980))).

22. NATHAN MILLER, *SPYING FOR AMERICA* 5 (1989).

23. Letter from George Washington to Lord Stirling (Oct. 6, 1778), in 13 *THE WRITINGS OF GEORGE WASHINGTON FROM THE ORIGINAL MANUSCRIPT SOURCES, 1745–99*, at 39 (John C. Fitzpatrick ed., 1936); *see also* Hayden, *supra* note 3, at 258 (discussing the importance of sharing information that appears to be of little or no intelligence value).

24. Many factors besides sharing breakdowns contribute to faulty intelligence, including analysts’ cognitive biases, the “crying-wolf effect” of past false alarms, and so on. *See* POSNER, *supra* note 1, at 85–86; RICHARD A. POSNER, *UNCERTAIN SHIELD: THE U.S. INTELLIGENCE SYSTEM IN THE THROES OF REFORM* 22–29 (2006). Even if data had flowed freely in the months before the 9/11 attacks, it’s far from clear that officials would have overcome these other obstacles to make the right intelligence calls. *See* MARK M. LOWENTHAL, *INTELLIGENCE: FROM SECRETS TO POLICY* 256–57 (4th ed. 2009). Enhanced information sharing may help stave off intelligence failure, but it doesn’t guarantee success.

25. Stewart A. Baker, *Should Spies Be Cops?*, *FOREIGN POL’Y*, Winter 1994–1995, at 36, 43.

our failure to anticipate the attack on Pearl Harbor.²⁶ In the months before December 1941, American cryptologists had broken the principal code for Japan's diplomatic communications and intercepted a number of increasingly alarming messages that Japan regarded conflict with the United States as inevitable.²⁷ Intelligence officers also determined that Japan had changed its naval call signs on November 1 and again on December 1, moves that were regarded "as signs of major preparations for some sort of Japanese offensive."²⁸ Yet these clues about Japan's possible intentions were never pooled and integrated:

[N]o single person or agency ever 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 channels of communication, some were blocked by technical or procedural delays; some never reached a center of decision.²⁹

Information sharing is also advantageous because it allows intelligence agencies to specialize in collecting different kinds of data, thereby producing efficiency gains. Consider the alternative: a system in which agencies only gain access to information they've collected 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 intercept electronic communications within the United States would be diverted to replicating NSA overseas signals-intelligence assets. Those inefficiencies mean less intelligence would be produced. (This is not a mere hypothetical. When NSA officials in 2001 refused to hand over intercepts of Osama Bin Laden's satellite telephone calls, the FBI made plans to conduct electronic surveillance by building its own antennae in Palau and Diego Garcia.³⁰) By contrast, an intelligence system based on information sharing allows agencies to carve out their own market niches. Agencies can focus their collection efforts on areas where they enjoy a comparative advantage—for example, the FBI's comparative advantage in gathering information relating to domestic crimes, the CIA's comparative advantage in gathering data from overseas spies, and so on. Sharing ensures that agencies will not 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 system's overall costs of producing intelligence assessments.

26. ROBERTA WOHLSTETTER, *PEARL HARBOR: WARNING AND DECISION* 277–78 (1962).

27. *Id.* at 382, 385–86.

28. *Id.* at 385.

29. *Id.* But see David Kahn, *The Intelligence Failure of Pearl Harbor*, *FOREIGN AFF.*, Winter 1991, at 138, 148 ("The intelligence failure at Pearl Harbor was not one of analysis, as Wohlstetter implies, but of collection.").

30. WRIGHT, *supra* note 2, at 344.

Sharing also has the potential to encourage “competitive analysis,”³¹ which can result in better advice to policy makers. In particular, sharing increases the number of agencies capable of engaging in what’s known as “all source intelligence.” All source means that an agency’s analytical products incorporate data from many different collection sources, not just the ones over which that particular agency has control.³² Three such entities currently exist (the CIA, the Defense Intelligence Agency, and the State Department’s Bureau of Intelligence and Research³³); information sharing can lead to the emergence of others. Sharing enables analysts to examine the widest possible range of information, including data gathered by other agencies. The result is a system of competitive analysis in which multiple agencies consult a common pool of information to tackle the same intelligence questions. The previous paragraph argued that redundant intelligence collection is inefficient, but not all redundancy is wasteful;³⁴ cars come 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 e-mail.³⁵ But redundant intelligence analysis can be beneficial. Competitive analysis helps ensure that policy makers are exposed to diverse perspectives; it also helps counteract groupthink tendencies.³⁶

Information sharing may produce even greater benefits in conflicts with terrorists than in traditional warfare between nation-states.³⁷ Indications that a conventional attack is imminent are comparatively easy to detect; it isn’t hard to figure out what the Soviets have in mind when they mobilize 20,000

31. See LOWENTHAL, *supra* note 24, at 14 (explaining that “competitive analysis” is “based on the belief that by having analysts in several agencies with different backgrounds and perspectives work on the same issue, parochial views more likely will be countered—if not weeded out—and proximate reality is more likely to be achieved”). Intelligence agencies “compete” in the sense that they vie with one another to produce the analytical outputs—threat assessments, reports, etc.—on which senior decision makers rely. In other words, agencies compete for more influence over policy makers, more prestige among their peers, and, to a lesser extent, enhanced budgets. See Sales, *supra* note 13, at 305.

32. See LOWENTHAL, *supra* note 24, at 72.

33. *Id.* at 38.

34. See Anne Joseph O’Connell, *The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post-9/11 World*, 94 CAL. L. REV. 1655, 1675–84 (2006) (discussing some costs and benefits of redundancy among intelligence agencies).

35. See *id.* at 1679–80 (arguing that redundant information collection can increase costs without providing proportional benefits).

36. See LOWENTHAL, *supra* note 24, at 14, 139; William C. Banks, *And the Wall Came Tumbling Down: Secret Surveillance After the Terror*, 57 U. MIAMI L. REV. 1147, 1151, 1193 (2003); O’Connell, *supra* note 35, at 1676, 1689, 1731–32. Competitive analysis also has its downsides. “The existence of an alternative analysis, especially on controversial issues, can lead policy makers to shop for the intelligence they want or cherry-pick analysis, which also results in politicization.” LOWENTHAL, *supra* note 24, at 135.

37. See Swire, *supra* note 3, at 955–57 (discussing the changed landscape of warfare and its effect on intelligence).

tanks to the border of West Germany.³⁸ But asymmetric warfare often involves precursor acts that by themselves appear innocent.³⁹ The warning signs of a terrorist attack could be as innocuous as a Nigerian named Umar Farouk Abdulmutallab boarding a Detroit-bound flight in Amsterdam on Christmas Day.⁴⁰ Their sinister implications can only be discerned when integrated with other pieces of information—for example, intercepts suggesting that al Qaeda intended to use a Nigerian to attack the United States around the holidays, intercepted e-mail traffic between Abdulmutallab and an anti-American cleric in Yemen, and warnings from Abdulmutallab's father that his son had become radicalized.⁴¹ 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.⁴²

Widespread data exchange has its benefits, but it also can harm the government's national security interests in several ways. Sharing increases the likelihood that sensitive intelligence will be compromised, whether through espionage (acquisition by a foreign power) or through leaks (disclosures to unauthorized persons, such as the news media).⁴³ The more 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 services. But in both cases there is a compelling safety rationale."⁴⁴

Still, the risk that sharing might compromise sensitive data seems exaggerated. Cold War Era information-access standards such as compartmentalization rules and "need to know" requirements were designed to counter a particular type of threat: espionage by a traditional nation-state adversary such as the Soviet Union.⁴⁵ They may be less vital in today's

38. See *id.* at 957 ("One important feature of the Cold War was that enemy mobilization was often graduated and visible.").

39. See LOWENTHAL, *supra* note 24, at 133.

40. See Mark Hosenball et al., *The Radicalization of Umar Farouk Abdulmutallab*, NEWSWEEK, Jan. 11, 2010, at 37 (discussing Abdulmutallab's personal background and the steps he took in his failed bombing attempt); Eric Lipton et al., *Review of Jet Bomb Plot Shows More Missed Clues*, N.Y. TIMES, Jan. 17, 2010, at A1 (detailing intelligence failures in connection with the 2009 Christmas Day terrorist plot).

41. Hosenball et al., *supra* note 41, at 37.

42. See Hayden, *supra* note 3, at 258 (arguing that pooling "the data points of human intelligence, imagery, or law enforcement" could result in "information of high value to national security").

43. See POSNER, *supra* note 1, at 102–04 (recounting concerns about sharing information).

44. *Id.* at 103.

45. See Mark A. Chinen, *Secrecy and Democratic Decisions*, 27 QUINNIPIAC L. REV. 1, 28–29 (2009) (claiming that compartmentalization and similar policies were adopted in response to the Cold War).

asymmetric conflicts with international terrorists.⁴⁶ Sharing restrictions still play an important role in preventing espionage by rival nations, such as Iran or North Korea.⁴⁷ But terrorist groups like al Qaeda have not proven as adept at placing spies in the American Intelligence Community.⁴⁸ At least as to information related to terrorist threats, then, the risks of espionage seem weaker. Of course, the danger that classified terrorism-related information might leak remains significant. Witness, for example, newspaper stories about the NSA's warrantless Terrorist Surveillance Program, secret CIA prisons in Central Europe, and so on.⁴⁹ But it might be possible to mitigate the risks of espionage and leaks with countermeasures other than sharing restrictions, such as electronic audit trails that record which officials have accessed a particular piece of information.⁵⁰

Sharing also can harm national security by producing a "flooding effect"—by inundating analysts with massive amounts of information.⁵¹ Roberta Wohlstetter argues that intelligence analysis is akin to trying to locate a faint "signal" hidden amid a mass of "noise."⁵² Information sharing can increase the amount of noise, making the signals even harder to detect. Sharing thus can overwhelm analysts, preventing them from detecting threats they otherwise would have found if only they hadn't been swamped with data.⁵³ Even worse, the flooding effect can lead to analytical distortions. By deluging analysts with unmanageable troves of data, sharing can reinforce their preconceptions about hostile powers' capabilities and intentions and blind them to unexpected threats.⁵⁴ In other words, sharing can exacerbate

46. *See id.* (suggesting that Cold War Era information-access policies are not as effective in conflicts with terrorists).

47. *See* David Morgan, *U.S. Adopts Preemptive Counterintelligence Strategy*, WASH. POST, Mar. 6, 2005, at A7 (reporting on new counterintelligence measures that were implemented to frustrate espionage efforts by China, Russia, Iran, North Korea, Cuba, and Libya).

48. *See* POSNER, *supra* note 24, at 215 (stating that terrorist organizations have less sophisticated intelligence operations than foreign states). *But see* Richard A. Opiel, Jr. et al., *Suicide Bomber in Afghanistan Was a Double Agent*, N.Y. TIMES, Jan. 5, 2010, at A1 (reporting that an al Qaeda suicide bomber who killed seven CIA officers at a CIA base in Afghanistan was a double agent).

49. *See, e.g.*, Dana Priest, *CIA Holds Terror Suspects in Secret Prisons*, WASH. POST, Nov. 2, 2005, at A1 (revealing the CIA's covert prison system for some al Qaeda captives); James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1 (reporting the existence of an NSA program to eavesdrop on certain international communications without court orders).

50. *See* MARKLE FOUND., *MOBILIZING INFORMATION TO PREVENT TERRORISM: ACCELERATING DEVELOPMENT OF A TRUSTED INFORMATION SHARING ENVIRONMENT* 7–8 (2006) (touting the benefits of certain defenses against leaks, such as electronic audit trails).

51. POSNER, *supra* note 1, at 104.

52. WOHLSTETTER, *supra* note 26, at 387, 393.

53. *See id.* at 387 (explaining that data overload can cause intelligence officers to sift through "all sorts of information that is useless and irrelevant").

54. *See* POSNER, *supra* note 1, at 116–17 (arguing that analysts respond to voluminous data by using their preconceptions to filter it).

confirmation bias.⁵⁵ Analysts might cope with the reams of new information by fixating on the data points that confirm their preexisting biases and ignoring the ones that do not.⁵⁶ The result is analytical ossification, as established theories are reinforced and alternatives go unnoticed.⁵⁷

Concerns about flooding are legitimate, but they don't justify wholesale limits on information sharing. It is 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.⁵⁸ The decisive factor is likely to be a rival agency's self-serving determination about whether the exchange would benefit its interests or harm them.⁵⁹ 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 rely on automated filtering technologies. The CIA reportedly is developing image-recognition technology that enables computers to match photographs with exemplars stored in a database.⁶⁰ The Office of the Director of National Intelligence also is said to be experimenting with an automated system that can scan databases of foreign surveillance videos and identify suspicious behavior.⁶¹ And computers are often tasked with running keyword queries ("al Qaeda," "jihad," and the like) against intercepted phone calls and e-mails.⁶² 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.")⁶³

It's not just the government that stands to lose from data exchange; sharing also can harm the privacy interests of the persons to whom the data relates.⁶⁴ Specifically, information sharing interferes with one's interest in preventing the government from observing personal facts.⁶⁵ The sharing of

55. *Id.* at 121.

56. *Id.*

57. *Id.*

58. *See supra* note 13 and accompanying text.

59. *See id.*

60. *See* LOWENTHAL, *supra* note 24, at 73.

61. Walter Pincus, *Finding a Way to Review Surveillance Tape in Bulk*, WASH. POST, Mar. 10, 2009, at A11.

62. *See, e.g.*, Michael Hirsh, *The NSA's Overt Problem*, WASH. POST, Jan. 1, 2006, at B1 (bemoaning the NSA's "primitive" technique of running random keyword searches for Islamist taglines).

63. LOWENTHAL, *supra* note 24, at 117.

64. *But cf.* Kris, *supra* note 3, at 520 (arguing that sharing restrictions "do[] not provide much protection for privacy").

65. *See, e.g.*, Julie E. Cohen, *Examined Lives, Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1371, 1375 (2000) ("'[P]rivacy' might encompass an enforceable right to prevent the sharing of . . . personally-identified data . . .").

previously collected data amounts to fresh observation in several senses. First, sharing increases the number of officials with access to an otherwise private fact; the more officials who observe it, the greater the privacy harms.⁶⁶ Second, and more importantly, information sharing enables the government to integrate isolated units of data and thereby discover new information about the person:

[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.⁶⁷

This is the same insight that informs the mosaic theory: integration creates new information.⁶⁸ Just as 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.

Besides harming one's privacy interest in avoiding unwanted observation, information sharing also can undermine one's privacy interest in controlling data about oneself. Sharing interferes with the ability of data subjects to manage the dissemination of personal information and, ultimately, how they choose to present themselves to the outside world:

What advocates regard as being fundamentally at stake in the claim to informational privacy is *control* of personal information. . . . [T]o speak of a right of informational privacy is to invoke a "claim of individuals . . . to determine for themselves when, how, and to what extent information about them is communicated to others."⁶⁹

The problem here is not so much that information sharing prevents data subjects from keeping personal information confidential; the problem is that

66. Cf. *Whalen v. Roe*, 429 U.S. 589, 602–03 (1977) (recognizing that the right to information privacy is threatened by increased exposure of that information).

67. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 507 (2006); cf. Patricia L. Bellia, *The Memory Gap in Surveillance Law*, 75 U. CHI. L. REV. 137, 139 (2008) (arguing that data retention and aggregation practices "threaten to convert many of the government surveillance activities now subject to a warrant requirement into the sort of 'indirect' surveillance at issue in—and unprotected by—[*United States v. Miller*], 425 U.S. 435 (1976)"]).

68. See *supra* text accompanying notes 17–20 (describing the mosaic theory).

69. Lillian R. BeVier, *Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection*, 4 WM. & MARY BILL RTS. J. 455, 458–59 (1995) (emphasis omitted) (quoting ALAN WESTIN, *PRIVACY AND FREEDOM* 7 (1967)); see also Francesca Bignami, *Towards a Right to Privacy in Transnational Intelligence Networks*, 28 MICH. J. INT'L L. 663, 669 (2007) (arguing that "when government agencies collect, combine, and manipulate information on individuals without their consent, they breach" the "essential liberal duty" of respecting citizens' choices "to keep certain matters private and to make other matters public").

sharing has the potential to undermine data subjects' autonomy.⁷⁰ Still, while it's certainly the case that information sharing can undermine privacy, sharing actually has the potential to promote privacy interests. This is so because, as I argue below, in some circumstances sharing can be a substitute for fresh privacy-eroding surveillance.⁷¹

Walls: Past and Present

The USA PATRIOT Act may have brought down one wall, but others remain on the statute books. This section begins with a brief discussion of the FISA wall and its underlying policy concerns. It then surveys several remaining statutory information-sharing limits. The National Security Act of 1947 might prevent the CIA from sharing information with federal law enforcement agencies—most notably the FBI—as well as other counterterrorism officials who operate primarily in the domestic sphere. The Posse Comitatus Act could result in federal criminal liability for members of the Armed Forces who exchange data or otherwise coordinate with law enforcement officials. Finally, the Privacy Act might restrict any federal agency from sharing with intelligence officials unless its reasons for handing over the data are sufficiently similar to the reasons it gathered the information in the first place.⁷²

70. See James X. Dempsey & Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459, 1462 (2004) (explaining that, in certain contexts, “privacy is about control, fairness, and consequences, rather than simply keeping information confidential”).

71. See *infra* subpart III(D).

72. See *supra* text accompanying note 12. Several other statutes have the potential to restrict information sharing, but do not have that effect at present because of how they are implemented. For instance, the Trade Secrets Act makes it a crime for federal officials to disclose virtually any kind of confidential business information—a restriction that could impede the free flow of data about vulnerabilities at critical infrastructure facilities like chemical plants. See 18 U.S.C. § 1905 (2006) (prohibiting any “officer or employee of the United States” from “publish[ing], divulg[ing], disclos[ing], or mak[ing] known in any manner or to any extent” any “information [that] concerns or relates to the trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association”). Yet the Trade Secrets Act contains an important exception: it permits disclosures that are otherwise “authorized by law.” *Id.* And the Homeland Security Act of 2002 authorizes intelligence agencies to exchange critical infrastructure information. Pub. L. No. 107-296, §§ 214(e)(1), (2)(D), 116 Stat. 2135, 2154 (codified at 6 U.S.C. §§ 133(e)(1), (2)(D) (2006)). The regulations implementing this directive state that DHS may provide

[Protected Critical Infrastructure Information] to an employee of the Federal government, provided . . . that such information is shared for purposes of securing the critical infrastructure or protected systems, analysis, warning, interdependency study, recovery, reconstitution, or for another appropriate purpose including, without limitation, the identification, analysis, prevention, preemption, and/or disruption of terrorist threats to the homeland.

6 C.F.R. § 29.8(b) (2010); see also *Chrysler Corp. v. Brown*, 441 U.S. 281, 312–13 (1979) (holding that validly promulgated regulations can amount to legal authorization within the meaning of the Trade Secrets Act). Similarly, the Health Insurance Portability and Accountability Act of 1996—which Congress enacted to ensure the privacy of personal medical records—conceivably could limit the sharing of information about victims of a bioterrorism attack or a pandemic. See Peter P. Swire & Lauren Steinfeld, *Security and Privacy After September 11: The Health Care Example*, 86 MINN.

Each of these statutes reflects a distinct set of policy values. Some laws seek to prevent pretext—the danger that criminal investigators might try to take advantage of the more flexible legal standards that govern surveillance for intelligence purposes. Others reflect firewall concerns; it might be appropriate to use certain military and intelligence practices in the foreign sphere, but those aggressive practices have no place here at home. A third principle is republicanism—the notion that the Armed Forces must always be kept firmly under the control of civilian authorities. Finally, there’s the good of privacy; the idea is to limit the government’s ability to engage in unwanted observation, as well as to respect the data subject’s ability to control the manner in which his information is presented to others.

A few qualifications are needed. First, I don’t mean to suggest that pretext, firewall, republicanism, and privacy concerns were foremost in Congress’s collective mind when it enacted the laws in question. Sometimes they were (the Privacy Act quite obviously was intended to preserve individual privacy), but sometimes they were not (the Posse Comitatus Act in particular comes to mind⁷³). My claim, rather, is that the statutes have the effect of vindicating these values in the present day.

Second, whether or not a given statute prohibits a particular kind of data exchange will rarely be an open-and-shut case. However, the fact that these laws do not unambiguously rule out information sharing is not cause for celebration. Legal uncertainty may be enough to halt data exchange. Risk-averse bureaucrats facing legal commands of unclear meaning may play it safe because they fear that a statutory violation—or even an allegation that a statute has been violated—will result in significant harms.⁷⁴ Officers who share information in violation of the law can expose themselves and their agencies to civil fines and even jail time. Statutory violations can produce less tangible harms as well. Public knowledge that an agency has violated its statutory charter can demoralize employees, decreasing their productivity. It can render the agency politically radioactive, resulting in the President and other senior policy makers keeping it at arm’s length. And it can encourage bureaucratic rivals to poach a weakened agency’s turf.⁷⁵ In short, it doesn’t

L. REV. 1515, 1525 (2002). However, the HIPAA privacy rule, promulgated by the Department of Health and Human Services in 2000, does not represent much of an obstacle. The privacy rule is understood to regulate only the flow of data from health-care providers to the government, not the flow of data among government agencies. *Id.* at 1528–29. And, in any event, the rule contains a number of exceptions that would permit information sharing in the event of a bioterrorism incident. *See, e.g.*, 45 C.F.R. §§ 164.512(b), (f), (j) (2009) (exceptions for “public health activities,” “law enforcement purposes,” and “avert[ing] a serious threat to health or safety”).

73. *See infra* notes 151–53 and accompanying text.

74. *See* MARKLE FOUND., *supra* note 51, at 32 (arguing that information-sharing guidelines must mitigate intelligence officials’ risk aversion).

75. Some of these harms may have befallen the CIA in the wake of allegations that the Agency violated domestic and international laws against torture when it subjected al Qaeda leaders to coercive interrogations, including waterboarding. The CIA lost some of its pull with the White House—witness the administration’s decision, over CIA objections, to release Justice Department

take a clear prohibition to gum up the works; information sharing can be thwarted nearly as easily by ambiguous legal commands that inspire risk-averse officials to shy away from the legal limits.

The Life and Times of the FISA Wall

The most notorious wall traces its roots to an obscure provision in FISA.⁷⁶ Enacted in 1978 against the backdrop of the Church Committee's explosive allegations of illegal wiretaps, suppression of dissent, and other systematic abuses in the Intelligence Community, FISA put an end to the Executive Branch's practice of conducting national security surveillance unilaterally. Henceforth the executive would need to apply to a special tribunal, known as the FISA Court or FISC, and establish to a judge's satisfaction that surveillance was legally justified.⁷⁷ Among various requirements, FISA directed the government to certify to the court that the "purpose" of the proposed surveillance was to gather foreign intelligence.⁷⁸ The basic idea was that if the government's central aim was to protect against foreign threats, it could avail itself of FISA's relatively lax surveillance standards.⁷⁹ If, on the other hand, the government's objective was principally to enforce domestic criminal laws, it would have to satisfy the relatively strict standards that govern garden-variety criminal investigations.⁸⁰ At some point in the 1980s, the Department of Justice (DOJ) began to read FISA as requiring that "the primary purpose" of the proposed surveillance must be to collect foreign intelligence.⁸¹ (The source of that test was the Fourth Circuit's decision in a pre-FISA case holding that warrantless electronic surveillance is permissible under the Fourth Amendment so long as its primary purpose is to gather foreign intelligence.⁸²)

How did one determine the government's purpose in a given case? By measuring the amount of coordination between intelligence officials and their law enforcement counterparts.⁸³ The more information that changed hands

memoranda on the legality of coercive interrogation. Mark Mazzetti & Scott Shane, *Memos Spell Out Brutal C.I.A. Mode of Interrogation*, N.Y. TIMES, Apr. 17, 2009, at A1. And the CIA's responsibility for interrogating senior al Qaeda captives was reassigned to the interagency High-Value Detainee Interrogation Group, or "HIG," which is led by the FBI. Anne E. Kornblut, *New Unit to Question Key Terror Subjects*, WASH. POST, Aug. 24, 2009, at A1.

76. For a detailed history of the FISA wall, see, for example, 9/11 COMMISSION REPORT, *supra* note 2, at 78–80; Kris, *supra* note 3, at 499–518.

77. See 50 U.S.C. § 1804 (2006) (establishing procedures for judicial orders approving electronic surveillance).

78. See *id.* § 1804(a)(7)(B).

79. See *In re Sealed Case*, 310 F.3d 717, 724–25 (FISA Ct. Rev. 2002) (analyzing the legislative history of FISA and highlighting the possibility that intelligence gathering and law enforcement may overlap in certain areas).

80. See *id.* at 725 (noting that "Congress was concerned about the government's use of FISA surveillance to obtain information not truly intertwined with the government's efforts to protect against threats from foreign powers").

81. See *id.* at 722 (discussing the development of the primary purpose test).

82. *United States v. Truong Dinh Hung*, 629 F.2d 908, 915 (4th Cir. 1980).

83. Kris, *supra* note 3, at 499–501.

between cops and spies, the more likely it was that the FISA Court would deem the primary purpose of the investigation to be something other than collecting foreign intelligence.⁸⁴ And that would take FISA's relatively liberal surveillance tools off the table.

In 1995, the Justice Department made it official; the agency issued a pair of directives that effectively segregated FBI intelligence officials from criminal investigators at the Bureau and at Main Justice.⁸⁵ The aim of the guidelines was to "clearly separate the counterintelligence investigation from the more limited . . . criminal investigations," thereby preventing any "unwarranted appearance that FISA is being used to avoid procedural safeguards which would apply in a criminal investigation."⁸⁶ DOJ therefore directed that information uncovered in the course of intelligence investigations—"including all foreign counterintelligence relating to future terrorist activities"—generally "will not be provided either to the criminal agents, the [U.S. Attorney's office], or the Criminal Division."⁸⁷ As a result, information sharing essentially ground to a halt.⁸⁸

The FISA wall thus was not just a statutory restriction; it also derived from administrative and judicial interpretations of the underlying statute. Why was it built in the first place? As the DOJ's 1995 guidelines indicate, the justification was the need to prevent officials from evading the legal limits on domestic surveillance.⁸⁹ Relatedly, officials wanted to keep the FISA Court from rejecting surveillance applications on the ground that cops' participation in an intelligence investigation had so contaminated it as to rule out FISA wiretaps.⁹⁰ Let's call this a pretext concern. (By maintaining the legal limits on domestic surveillance, the FISA wall also sought to preserve

84. *Id.* at 497–99.

85. *See, e.g.*, Memorandum from Jamie S. Gorelick, Deputy Attorney Gen., to Mary Jo White, U.S. Attorney, S. Dist. N.Y. et al. 2 [hereinafter Gorelick Memo], available at <http://www.cnss.org/1995%20Gorelick%20Memo.pdf>; Memorandum from Janet Reno, Attorney Gen., to Assistant Attorney Gen. et al. § (A)(6) (July 19, 1995) [hereinafter Reno Memo], available at <http://www.fas.org/irp/agency/doj/fisa/1995procs.html>.

86. Gorelick Memo, *supra* note 85, at 2.

87. *Id.* at 2, 3.

88. *See In re Sealed Case*, 310 F.3d 717, 728 (FISA Ct. Rev. 2002) (noting that although the "procedures provided for significant information sharing and coordination . . . , they eventually came to be narrowly interpreted . . . as requiring . . . a 'wall' to prevent the FBI intelligence officials from communicating with the Criminal Division regarding ongoing [foreign intelligence] investigations").

89. *See* U.S. GEN. ACCOUNTING OFFICE, FBI INTELLIGENCE INVESTIGATIONS: COORDINATION WITHIN JUSTICE ON COUNTERINTELLIGENCE CRIMINAL MATTERS IS LIMITED 17 (2001) (explaining that the Reno Memo was designed "to establish a process to properly coordinate DOJ's criminal and counterintelligence functions and to ensure that intelligence investigations were conducted lawfully").

90. *See id.* at 12 (discussing FBI officials' concern that interaction with criminal investigators regarding an intelligence investigation might cause the FISA Court to deny a FISA surveillance application).

the privacy interests of persons subject to surveillance. A good deal more will be said about privacy below.⁹¹⁾

The risk of pretextual surveillance arises from differences in the respective rules under which intelligence and law enforcement surveillances are carried out. The constitutional and statutory standards that govern the former are weaker than the rules applicable to the latter.⁹² The federal wiretap statute—known in the trade as “Title III”—provides that law enforcement officials generally may not conduct surveillance unless they obtain a “superwarrant.”⁹³ In addition to showing that they are taking steps to minimize the acquisition of innocent conversations and that they have exhausted alternative investigative techniques, officials must establish probable cause to believe a crime has been, is being, or is about to be committed.⁹⁴ By contrast, FISA only requires intelligence investigators to establish probable cause that the target is a “foreign power” or an “agent of a foreign power”⁹⁵—in layman’s terms, a spy or a terrorist. The standards are looser still for intelligence collection overseas.⁹⁶ The Fourth Amendment may not apply to noncitizens who are not present in the United States—not only the warrant requirement, but also the requirement of reasonableness.⁹⁷ And many surveillance statutes don’t apply to intelligence gathering in foreign countries at all, or at least apply differently than they do here at home.⁹⁸

Those disparate standards create arbitrage opportunities. Officials who are bound by relatively rigorous surveillance rules might look for ways to take advantage of comparatively flabby collection standards. In particular, law enforcement officers might prefer for their wiretaps to be run by counterparts in the Intelligence Community, who would then share the

91. See *infra* subparts II(D) and III(D).

92. See Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 620 (2003) (comparing the legal thresholds for government surveillance); cf. *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 322 (1972) (citing “potential distinctions” between “criminal surveillances and those involving the domestic security”).

93. Kerr, *supra* note 93, at 645.

94. 18 U.S.C. §§ 2518(3)(a), (3)(c), (5) (2006).

95. 50 U.S.C. §§ 1801(a)–(b), 1805(a)(3) (2006).

96. See *id.* § 1881a(a) (allowing the Attorney General and the Director of National Intelligence to jointly authorize the “targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information”).

97. See, e.g., *United States v. Verdugo-Urquidez*, 494 U.S. 259, 261–65 (1990) (holding that the Fourth Amendment does not extend to searches and seizures of property owned by nonresidents and located in a foreign country). *But cf.* *Boumediene v. Bush*, 128 S. Ct. 2229, 2255–58 (2008) (establishing a “functional test” to determine whether aliens detained outside of the United States have a constitutional right to seek writs of habeas corpus).

98. James Risen & Eric Lichtblau, *Court Affirms Wiretapping Without Warrants*, N.Y. TIMES, Jan. 16, 2009, at A13.

intercepts for use in criminal investigations.⁹⁹ Cops might, in other words, issue tasking orders to spies; they might delegate their responsibilities for criminal surveillance to surrogates in the Intelligence Community. To put matters differently, there could be a substitution effect. If the cost of ordinary criminal surveillance (measured in part by the difficulty of establishing the necessary legal predicates) is excessive, investigators will want to switch to lower cost surveillance techniques. To the extent that intelligence surveillance requires less in the way of predication—a weaker probable cause standard in the domestic sphere, and maybe not even reasonableness in the foreign sphere—law enforcement officials may regard it as a less costly, and therefore more attractive, alternative.

The FISA wall helped prevent this substitution from taking place.¹⁰⁰ The wall effectively increased the cost of the substitute good—law enforcement surveillance conducted by intelligence officials—to infinity; there were no circumstances in which criminal investigators would be permitted to assign to intelligence operatives their responsibility for gathering evidence for use in prosecutions. Notice that the wall didn't just restrict cops from overtly tasking spies with surveillance; it also restricted informal interactions between cops and spies, such as collaborating on overlapping investigations and sharing information with each other.¹⁰¹ The FISA wall thus amounted to a prophylactic rule.¹⁰² In addition to regulating the specific harm that DOJ sought to avert (cops evading the legal limits on domestic surveillance by issuing tasking orders to spies), the wall also proscribed related conduct that could either be wholly innocent or could be the first tentative steps toward an impermissible tasking.¹⁰³

The wall eventually came down. Section 218 of the USA PATRIOT Act abolished the primary purpose test, substituting a new requirement that the government's goal of collecting foreign intelligence must be "a significant purpose" of proposed FISA surveillance.¹⁰⁴ As a result, FISA

99. See Baker, *supra* note 25, at 41–42 (describing the temptation for law enforcement officers to recast their investigations as intelligence operations to take advantage of looser standards).

100. See Sales, *supra* note 13, at 287–88 (describing how FISA prevented information sharing).

101. *Id.*

102. See, e.g., Brian K. Landsberg, *Safeguarding Constitutional Rights: The Uses and Limits of Prophylactic Rules*, 66 TENN. L. REV. 925, 926 (1999) (describing "prophylactic rules" as "risk-avoidance rules that are not directly sanctioned or required by the Constitution, but that are adopted to ensure that the government follows constitutionally sanctioned or required rules"); David A. Strauss, *The Ubiquity of Prophylactic Rules*, 55 U. CHI. L. REV. 190, 195 (1988) (defining "prophylactic rule" as a "rule that imposes additional requirements beyond those of the Constitution itself").

103. See Sales, *supra* note 13, at 288 (explaining that the FISA Court's requirement that it be informed of all contacts between cops and spies had a chilling effect on their interactions with each other).

104. USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 218, 115 Stat. 272, 291 (codified at 50 U.S.C. § 1804(a)(6)(B) (2006)). Section 203 of the PATRIOT Act eliminated two other statutory walls. It amended Federal Rule of Criminal Procedure 6(e) to authorize prosecutors to share grand jury information with various national security players, and it amended the federal wiretap statute to

would still be a viable option even if the government intended to use the resulting intercepts not just to, say, turn a suspected spy into a double agent (a classic counterespionage technique), but also to prosecute that spy for espionage (the textbook law enforcement move).¹⁰⁵ FISA would still be a viable option even if the spies and cops talked to one another about their respective approaches to the case.¹⁰⁶ Section 504 was even blunter; it provided that intelligence officials “may consult with Federal law enforcement officers to coordinate efforts” against national security threats.¹⁰⁷ Many academics take a dim view of these changes, arguing that PATRIOT enables officials to engage in what I’m calling pretextual surveillance.¹⁰⁸ The FISA Court shared some of those concerns, but in 2002 the FISA Court of Review upheld the amended FISA against a constitutional challenge.¹⁰⁹

National Security Act of 1947

The National Security Act of 1947 represents another potentially significant barrier to information sharing. That landmark legislation, enacted in the wake of the Allied victory in World War II and with the Cold War faintly visible on the horizon, established the Central Intelligence Agency,¹¹⁰ granting the Agency certain powers and denying it certain others.¹¹¹ As

authorize criminal investigators to share intercepts with various national security players. See generally 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) (summarizing the changes to Rule 6(e) adopted in the USA PATRIOT Act).

105. Kris, *supra* note 3, at 498 (“[A] FISA wiretap conducted for a law enforcement purpose, such as prosecuting a spy for espionage, would typically be indistinguishable . . . from a FISA wiretap conducted for a traditional intelligence purpose, such as recruiting the spy as a double agent.”).

106. See *In re Sealed Case*, 310 F.3d 717, 734–35 (FISA Ct. Rev. 2002) (explaining that FISA, as amended by the USA PATRIOT Act, allows greater coordination between intelligence and law enforcement officials).

107. USA PATRIOT Act § 504.

108. See, e.g., Banks, *supra* note 37, at 1149 (“As it now stands, the government may take advantage of the secretive and less protective procedures of FISA to plan and carry out surveillance and searches of American citizens, without giving notice or conducting any proceeding before a magistrate.”); Erwin Chemerinsky, *Losing Liberties: Applying a Foreign Intelligence Model to Domestic Law Enforcement*, 51 UCLA L. REV. 1619, 1624 (2004) (“Already it is apparent that the federal government is using its powers under the Patriot Act in contexts that have nothing to do with terrorism.”); David Hardin, *The Fuss over Two Small Words: The Unconstitutionality of the USA Patriot Act Amendments to FISA Under the Fourth Amendment*, 71 GEO. WASH. L. REV. 291, 294 (2003) (arguing that “the new standard serves as an invitation for any proclivity that law enforcement authorities may have in abusing its surveillance authority under the guise of national security while diminishing the judiciary’s role in safeguarding personal rights against unreasonable law enforcement activity”); George P. Varghese, *A Sense of Purpose: The Role of Law Enforcement in Foreign Intelligence Surveillance*, 152 U. PA. L. REV. 385, 386 (2003) (calling into question the constitutionality of the PATRIOT Act’s “significant purpose” test).

109. *In re Sealed Case*, 310 F.3d at 746.

110. 50 U.S.C. § 403-4 (2006).

111. The CIA is granted the power to “collect intelligence through human sources and by other appropriate means” but denied any “police, subpoena, or law enforcement powers or internal security functions.” *Id.* § 403-4a(d)(1).

relevant here, the CIA is denied any “police, subpoena, or law enforcement powers or internal security functions.”¹¹² That notoriously ambiguous prohibition could impede the Agency’s efforts to share intelligence information with counterparts at the FBI or elsewhere in the law enforcement community, and also to receive data from them in return.¹¹³

At least two distinct policy judgments are reflected in the internal security ban. The first might be called a firewall concern. The idea is that, while it might be appropriate for intelligence officials to use aggressive and unsavory techniques overseas, the government should not operate the same way in the domestic sphere.¹¹⁴ Intelligence can be a dirty business. The enterprise involves breaking and entering, theft, eavesdropping on political leaders, kidnapping, unwitting application of mind-altering drugs, coercive interrogations, and the like—sometimes even murder and assassination.¹¹⁵ We might tolerate this sort of state-sanctioned violence if confined to faraway lands (though we might not). But no one thinks it should take place at home. Here, judicial checks on Executive Branch surveillance, seizures, and sanctions are the norm. The internal security ban thus functions as a barrier, preventing the tainted (but perhaps necessary) world of foreign intelligence operations from bleeding over into and contaminating the relatively pristine domestic world.

Commentators often posit that Congress adopted the internal security ban because it wanted to prevent the CIA from emulating the authoritarian German and Soviet intelligence systems.¹¹⁶ Memories of Nazi Germany’s notoriously ruthless police force—the Gestapo—were still fresh in 1947. More recent examples could be found behind the descending Iron Curtain, as Stalin began to export his special brand of police terror to his involuntary allies in Central and Eastern Europe.¹¹⁷ The standard account is true enough, but incomplete in one important respect. It doesn’t appear that Congress

112. *Id.*

113. See Harris, *supra* note 8, at 532–36 (discussing the 1947 Act’s “broad and sometimes vague terms”).

114. See, e.g., Kate Martin, *Intelligence, Terrorism, and Civil Liberties*, 29 HUM. RTS., Winter 2002, at 5, 5 (arguing that practices that would be dangerously intrusive domestically may be necessary in the war against terrorism).

115. See Roberto Suro, *FBI’s “Clean” Team Follows “Dirty” Work of Intelligence*, WASH. POST, Aug. 16, 1999, at A13 (explaining that the FBI uses separate teams to keep more “shocking” tactics confined to the intelligence realm).

116. See, e.g., Sherri J. Conrad, *Executive Order 12,333: “Unleashing” the CIA Violates the Leash Law*, 70 CORNELL L. REV. 968, 975 (1985) (discussing concerns that the CIA may “evolve into an American secret police”); Harris, *supra* note 8, at 531 (asserting that recent memories of World War II led to Congress carving out clear jurisdictional roles for intelligence agencies); Manget, *supra* note 1, at 416 (citing a “deep uneasiness” around the creation of the CIA); Daniel L. Pines, *The Central Intelligence Agency’s “Family Jewels”: Legal Then? Legal Now?*, 84 IND. L.J. 637, 640 (2009) (stating that Congress did not want the CIA to become another secret police).

117. See Michael Schwartz, *A Celebration is Haunted by the Ghost of Stalin*, N.Y. TIMES, May 8, 2010, at A9.

wanted to ban the use of aggressive intelligence techniques *per se*.¹¹⁸ It simply wanted to ban their use *inside the United States*. If Congress had the sweeping ambitions sometimes attributed to it, it could have fortified the CIA's statutory charter with express restrictions on kidnapping, assassination, or numerous other practices. It didn't. Instead, it chose to rule them out in connection with internal security, leaving external security essentially as it found it.¹¹⁹ That suggests Congress may have been content to give the CIA relatively free rein to operate overseas. Congress didn't care if the CIA was a "rogue elephant,"¹²⁰ as long as it was stampeding America's enemies rather than her citizens.

The ban on internal security functions serves a second policy value as well—preventing government officials from doing an end run around legal limits on domestic surveillance. This is identical to the FISA wall's *pretext* rationale discussed above.¹²¹ (Again, this anti-pretext provision also preserves the privacy interests of persons subject to surveillance. A good deal more will be said about privacy below.¹²²) If the CIA had internal security responsibilities, investigators might engage in pretextual surveillance—i.e., wiretaps whose superficial purpose is to collect information for intelligence purposes, but whose true objective is to gather evidence for use in a garden-variety criminal investigation. The internal security prohibition makes it harder for law enforcement officials to commission pretextual wiretaps. Because the CIA is statutorily barred from undertaking certain kinds of domestic operations, and perhaps even from sharing information concerning certain domestic operations, there are fewer opportunities for officials to evade the restrictive rules that govern criminal investigations.¹²³ (The seal is not watertight; Executive Order 12,333 authorizes the CIA to undertake a variety of domestic operations, such as protecting agency facilities and personnel against various threats.¹²⁴)

118. See Conrad, *supra* note 117, at 937 ("Congress designed the National Security Act to interdict domestic spying.").

119. See S. REP. NO. 94-755, at 56 (1976) (citing intelligence officials' testimony that the internal security restriction "was intended to 'draw the lines very sharply between the [Central Intelligence Group] and the FBI'" and that the "CIA would be limited definitely to purposes outside of the country").

120. See Editorial, *Let Congress Chain This Rogue Elephant*, DAYTONA BEACH MORNING J., Sept. 12, 1975, at 4A (reporting that Senator Frank Church called the CIA a "'rogue elephant' on a rampage without command").

121. See *supra* notes 90–110 and accompanying text.

122. See *infra* subparts II(D) and III(D).

123. See 50 U.S.C. §§ 401a(1), 403-4a(d) (2006) (limiting the breadth of CIA activities to foreign intelligence and counterintelligence).

124. Exec. Order No. 12,333, 3 C.F.R. 200 (1982), *as amended* by Exec. Order No. 13,284, 68 Fed. Reg. 4075 (Jan. 23, 2003), Exec. Order No. 13,355, 69 Fed. Reg. 53,593 (Aug. 27, 2004), Exec. Order No. 13,470, 73 Fed. Reg. 45,325 (Aug. 4, 2008), *reprinted as amended* in 50 U.S.C. § 401 (2006).

How does the 1947 Act give concrete form to these firewall and pretext concerns? Badly. The terms of the statutory prohibition on “police, subpoena, or law enforcement powers or internal security functions”¹²⁵ are notoriously ambiguous. In 1976, the Church Committee criticized the phrase’s indeterminacy.¹²⁶ Modern observers haven’t been much kinder. One scholar berates Congress for “failing to use clear and unambiguous language restricting internal operations by the CIA,”¹²⁷ and even the Agency’s former general counsel confesses that “the limits of what the CIA can and cannot do are not clear.”¹²⁸ Nor has the judiciary offered much assistance; “[c]ourts have generally eschewed clear definitions and parameters on CIA domestic activity.”¹²⁹ Because of its indeterminacy, the 1947 Act is amenable to any number of competing interpretations. A strict reading of “internal security,” championed by some,¹³⁰ would exclude the CIA from virtually any domestic responsibilities whatsoever.¹³¹ The flexible reading favored by others¹³² would preserve at least some domestic responsibilities for the agency.

Who’s right? The answer matters a great deal. Depending on how it is interpreted, the internal security ban could impose severe restrictions on information sharing between the CIA and the FBI and other domestic entities.¹³³ To be sure, the Agency and Bureau don’t need a statute to keep them from swapping data; as bitter bureaucratic rivals, they will have strong incentives to keep their information to themselves.¹³⁴ Yet legal restrictions can make matters worse.

For instance, the 1947 Act conceivably could prevent the FBI and CIA from mounting joint investigations of global terrorist groups. Imagine a terrorist outfit whose members are based overseas but who occasionally travel to the United States to raise money, case targets, and conduct operations; the group has both a domestic and an international presence. The

125. 50 U.S.C. § 403-4a(d)(1).

126. See FINAL REPORT OF THE SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, U.S. SENATE, INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK II, S. REP. NO. 94-755, at 96–98 (1976) (referring to the phrase’s “ambiguity”).

127. Conrad, *supra* note 117, at 971.

128. Harris, *supra* note 8, at 533 (quoting Jeffrey H. Smith, former CIA general counsel).

129. *Id.* at 534.

130. See, e.g., Conrad, *supra* note 117, at 973 & n.35, 975–76 (discussing how certain courts interpret the phrase “internal-security functions in a restrictive manner”).

131. See *id.* at 972–73 n.35 (criticizing Executive Order 12,333’s interpretation of the phrase “internal security” and arguing that “Congress prohibited all CIA domestic activity except for matters of CIA facility security and personnel”).

132. See Harris, *supra* note 8, at 547 (discussing how the Act’s ambiguity gives rise to flexible interpretations).

133. See Conrad, *supra* note 117, at 988 (arguing that the 1947 Act restricts the CIA from exchanging data with domestic entities).

134. See Sales, *supra* note 13, at 303–13.

Bureau and Agency might want to divide the labor: the CIA would surveil targets when they are abroad, the FBI would surveil any targets who happen to be within the United States, and they would hand off the baton as targets cross the border. The two agencies then would share their respective surveillance take with each other. (This is an example of how information sharing can reduce the need for redundant collection efforts, thereby promoting efficiency.) The 1947 Act might forbid the data exchange on which this sort of collaboration depends.

Consider the flow of information from the CIA to the FBI. The FBI isn't just responsible for domestic intelligence; it's also the nation's preeminent law enforcement agency.¹³⁵ That means the Bureau may want to use a given piece of information for intelligence purposes, but it also may want to use the same data in criminal proceedings; the information is "dual use."¹³⁶ Suppose the CIA hands the FBI intelligence information that it collected overseas. If the Bureau intends to use it in a criminal prosecution, the CIA becomes an active participant in the collection of evidence for use at trial.¹³⁷ The CIA effectively operates as the FBI's agent, exercising something like a delegated power to collect evidence of criminal activity. Does that count as the exercise of a "law enforcement power[]" within the meaning of the 1947 Act? The case that it does is by no means frivolous. Similar problems are evident when information flows in the opposite direction. May the Bureau give the CIA its dual-use information—i.e., data that was gathered partly for law enforcement purposes? The CIA's receipt of the data makes it a direct beneficiary of a core law enforcement function—collecting evidence of criminal wrongdoing—and that could be seen as participation in the exercise of a "law enforcement power[]." ¹³⁸

Even worse, the FBI's intentions may not be clear, and they may evolve over time. This is in essence a retroactivity problem. At the moment the CIA and the Bureau swap information; the two agencies may intend for it to be used only for intelligence purposes. But at some point the FBI might decide that the most effective way to proceed against a particular terrorist is to charge him with a crime. The guidelines that govern FBI operations recognize that these categories are fluid:

135. *New Attorney General Guidelines for Domestic Intelligence Collection: Hearing Before the S. Comm. on Intelligence*, 110th Cong. 1 (2008) (joint statement of Elisebeth Collins Cook, Assistant Att'y Gen. of the Office of Legal Policy, and Valerie Caproni, Gen. Counsel of the FBI).

136. See Michael B. Mukasey, *Where the U.S. Went Wrong on the Christmas Day Bomber*, WASHINGTONPOST.COM, Feb. 12, 2010, <http://www.washingtonpost.com/wp-dyn/content/article/2010/02/11/AR2010021103331.html> (explaining that the FBI seeks to protect the public from crimes and threats to national security, and to further foreign intelligence objectives).

137. Depending on the arrangement, the FBI might be barred from using CIA-originated information in criminal proceedings without the Agency's permission. Information-sharing agreements between agencies (or between nations) often include ORCON restrictions—that is, "originator controls"—that bar recipients from using the data in particular ways unless the originator consents. See LOWENTHAL, *supra* note 24, at 154.

138. 50 U.S.C. § 403-4a(d)(1) (2006).

[T]he FBI's information gathering activities [need not] be differentially labeled as "criminal investigations," "national security investigations," or "foreign intelligence collections," or that the categories of FBI personnel who carry out investigations be segregated from each other based on the subject areas in which they operate. Rather, all of the FBI's legal authorities are available for deployment in all cases to which they apply to protect the public from crimes and threats to the national security and to further the United States' foreign intelligence objectives.¹³⁹

An investigation that began life looking like an intelligence matter could reach maturity looking like a criminal matter, and vice versa. As a result, data exchange that was entirely unrelated to the criminal law when it took place could be retroactively converted, thanks to the FBI's latter-day shift in emphasis, into law enforcement activity that violates the 1947 Act.

The National Security Act could impede sharing in another way, too: by preventing the CIA from participating in operations to capture suspected terrorists abroad and bring them to the United States to stand trial. The Agency sometimes apprehends terrorists and others wanted by the FBI.¹⁴⁰ In the late 1990s, the CIA crafted a plan to kidnap Osama Bin Laden in Afghanistan; the Saudi was under indictment in the Southern District of New York for al Qaeda's 1998 bombing of two American embassies in East Africa, and a CIA snatch job would be the first step in bringing the terror master to justice.¹⁴¹ The CIA taking Bin Laden into custody might count as "law enforcement" within the meaning of the 1947 Act: the Agency essentially would be functioning as the FBI's delegate, performing the core law enforcement function of apprehending a fugitive so he can be brought before a court.¹⁴² The 1947 Act similarly might rule out information sharing about such apprehensions. Suppose the FBI itself captures Bin Laden after being tipped off by CIA analysts that he is hiding out at his Tarnak Farms compound in Afghanistan. Is it law enforcement for the CIA to share information it knows the FBI will use in connection with a criminal prosecution? What if, at the time of the capture, the government hasn't decided what it will do with Bin Laden once he's in custody? Criminal prosecution is an obvious option, but it's not the only one; Bin Laden might be held in military custody or held by the CIA for interrogation. Does the

139. THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS 7 (2008).

140. See David Stout, *C.I.A. Detainees Sent to Guantánamo*, NYTIMES.COM, Sept. 6, 2006, <http://www.nytimes.com/2006/09/06/washington/06cnd-bush.html> (describing the CIA's apprehension program).

141. See WRIGHT, *supra* note 2, at 265–66 (detailing a CIA plan to use Afghan tribesmen—who were leftover assets from the conflict with the Soviets—to kidnap Bin Laden, and describing the evidence used in the New York grand jury indictment).

142. See LOWENTHAL, *supra* note 24, at 188 (noting that renditions "require the presence of U.S. law enforcement personnel even if the operation is primarily an intelligence operation").

mere possibility of criminal proceedings convert the CIA's information sharing into "law enforcement" in violation of the 1947 Act?¹⁴³

Again, the point is not that the CIA's statutory charter clearly rules out these sorts of information-sharing arrangements. It doesn't. The scope of the ban on "police, subpoena, or law enforcement powers or internal security functions"¹⁴⁴ is not a model of clarity, and it's far from certain which types of data exchange are permitted and which are forbidden. But that is not a point in the statute's favor. Mere ambiguity can be enough to dissuade government officials from sharing information with one another, as they worry about whether doing so would land their agencies—or themselves—in hot water.

Posse Comitatus Act

The Posse Comitatus Act is a second possible source of information-sharing limits. Originally enacted in 1878, the Act makes it a crime for anyone "willfully [to] use[] any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws" except "in cases and under circumstances expressly authorized by the Constitution or Act of Congress."¹⁴⁵ *Posse comitatus* refers to the common law power of a sheriff to "summon [t]he entire population of a county above the age of 15 . . . as to aid him in keeping the peace, in pursuing and arresting felons."¹⁴⁶ The Posse Comitatus Act is one of the more venerated laws in the U.S. Code. It's also one of the more vexing, because its strict but ambiguous limits could interfere with information sharing between law enforcement authorities and the Armed Forces.¹⁴⁷

143. Section 905 of the USA PATRIOT Act might permit some of these information-sharing initiatives, but it isn't a slam dunk. The statute amends the 1947 Act by generally providing that the Attorney General, or the head of any other department or agency of the Federal Government with law enforcement responsibilities, shall expeditiously disclose to the Director of Central Intelligence . . . foreign intelligence acquired by an element of the Department of Justice or an element of such department or agency, as the case may be, in the course of a criminal investigation.

USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 905, 115 Stat. 272, 388–89 (codified at 50 U.S.C. § 403-5b, 5c (2006)). But § 905 has its limits. First, it doesn't authorize bilateral data exchange; it only permits sharing in one direction, from the law enforcement world to the CIA. *See id.* (requiring law enforcement agencies to disclose foreign intelligence to the CIA, but remaining silent on information transfer from the CIA to law enforcement agencies). It therefore wouldn't override any restriction in the 1947 Act on the CIA sending information to counterparts at law enforcement agencies. Second, and more importantly, § 905 only permits sharing "[e]xcept as otherwise prohibited by law." *Id.* That reservation clause might maintain any information-sharing limits required by CIA's statutory charter.

144. 50 U.S.C. § 403-4a(d)(1).

145. 18 U.S.C. § 1385 (2006).

146. DELUXE BLACK'S LAW DICTIONARY 1162 (6th ed. 1990); *see also* BLACK'S LAW DICTIONARY 1183 (8th ed. 2004) (defining *posse comitatus* as a "group of citizens who are called together to help the sheriff keep the peace or conduct rescue operations").

147. *See* Sales, *supra* note 13, at 329.

The Posse Comitatus Act vindicates two distinct policy values. The first is the familiar firewall concern—the notion that some national security operations ought not to be attempted in certain contexts even if they’re unobjectionable elsewhere.¹⁴⁸ The second might be called a republicanism concern—i.e., the longstanding American determination to preserve representative self-government, in part by securing civilian control of the Armed Forces.¹⁴⁹ I do not argue that firewall and republicanism values were at the top of Congress’s list of priorities when it passed the Posse Comitatus Act. To the contrary, the historical evidence suggests that the Reconstruction Congress enacted the legislation for odiously racist reasons.¹⁵⁰ The states of the former Confederacy objected to the use of federal troops to guarantee freedmen the right to vote and generally to prevent election fraud.¹⁵¹ In 1878 they managed to persuade the rest of Congress to enact their preferences into law.¹⁵² Whatever its origins, however, the Posse Comitatus Act today has come to stand for these two policy concerns.

Consider firewall principles first. The Posse Comitatus Act reflects the notion that the Armed Forces—more precisely, the Army and the Air Force (the Act doesn’t mention the Navy or Marines, though the Defense Department applies it to them as a matter of policy¹⁵³)—should be kept separate from the world of law enforcement.¹⁵⁴ The Act thus serves to insulate criminal investigations from the more violent practices and rules of engagement that characterize military operations.¹⁵⁵ This firewall concern is

148. See *supra* notes 115–31 and accompanying text.

149. See THE FEDERALIST NO. 8, at 67–70 (Alexander Hamilton) (Clinton Rossiter ed., 1961) (expressing concern that maintaining a large standing army can lead to oppression).

150. See, e.g., Gary Felicetti & John Luce, *The Posse Comitatus Act: Setting the Record Straight on 124 Years of Mischief and Misunderstanding Before Any More Damage Is Done*, 175 MIL. L. REV. 86, 90 (2003) (citing “the Act’s true origins in Reconstruction bitterness and racial hatred”).

151. *Id.* at 110.

152. See, e.g., Candidus Dougherty, “Necessity Hath No Law”: *Executive Power and the Posse Comitatus Act*, 31 CAMPBELL L. REV. 1, 12–14 (2008) (describing the long tension between southern states and Congress regarding freedmen’s rights, influencing the 1876 presidential election and resulting in passage of the Posse Comitatus Act in 1878); Felicetti & Luce, *supra* note 151, at 100–13.

153. See Michael Greenberger, *Did the Founding Fathers Do “A Heckuva Job”?* *Constitutional Authorization for the Use of Federal Troops to Prevent the Loss of a Major American City*, 87 B.U. L. REV. 397, 406 (2007).

154. See Felicetti & Luce, *supra* note 151, at 120 (citing a unanimous 1882 Senate Judiciary Committee report confirming the “primary evil addressed by the Posse Comitatus Act [as] the marshal’s power to call out and control the Army”).

155. *Effect of Posse Comitatus Act on Proposed Detail of Civilian Employee to the National Infrastructure Protection Center*, Memorandum from William Michael Treanor, Deputy Assistant Att’y Gen., Office of Legal Counsel, to the General Counsel, FBI (May 26, 1998), available at <http://www.justice.gov/olc/pca1fnl.htm> (“Relevant caselaw and opinions of [the Office of Legal Counsel] reflect the view that the PCA is intended to prohibit military personnel from directly coercing, threatening to coerce, or otherwise regulating civilians in the execution of criminal or civil laws.”).

similar to the rationale for Congress's decision in the National Security Act of 1947 to largely exclude the CIA from domestic operations.¹⁵⁶ But there is a subtle difference. The 1947 Act draws both a geographic line of demarcation (the CIA may operate overseas but not in the United States) and a functional one (the CIA may engage in intelligence but not law enforcement).¹⁵⁷ *Posse Comitatus*, by contrast, draws only a functional line. The Armed Forces may undertake military functions but they may not assume law enforcement responsibilities.¹⁵⁸

The underlying insight is that soldiers and cops have fundamentally different missions. The soldier's job is to kill the enemy; the cop's is to enforce the law.¹⁵⁹ The military subdues enemy forces through overwhelming violence.¹⁶⁰ Law enforcement doesn't have "enemies"; instead, officers encounter presumptively innocent fellow citizens who are entitled to a full panoply of constitutional rights, both substantive and procedural.¹⁶¹ Another important difference has to do with the permissibility of force. The default rule for soldiers on the battlefield is that they are entitled to use force, even deadly force.¹⁶² The default rule for cops on the beat is the opposite; they may use deadly force only in extreme circumstances, as when a suspect threatens the life of a police officer or a bystander.¹⁶³ Battlefield rules of engagement seek to maximize military effectiveness;¹⁶⁴ the rules governing criminal investigations seek to constrain, to prevent officers from investigating, arresting, and detaining too aggressively.¹⁶⁵ The *Posse Comitatus* Act thus prevents military mores and

156. See *supra* note 114 and accompanying text.

157. See *supra* note 114 and accompanying text.

158. See *supra* note 146 and accompanying text.

159. See DIANE CECILIA WEBER, CATO INST., WARRIOR COPS: THE OMINOUS GROWTH OF PARAMILITARISM IN AMERICAN POLICE DEPARTMENTS 10 (1999); William C. Banks, *The Normalization of Homeland Security After 9/11: The Role of the Military in Counterterrorism Preparedness and Response*, 64 LA. L. REV. 735, 771 (2004); Sean J. Kealy, *Reexamining the Posse Comitatus Act: Toward a Right to Civil Law Enforcement*, 21 YALE L. & POL'Y REV. 383, 386 (2003) (explaining crucial differences between military objectives and law enforcement objectives).

160. See WEBER, *supra* note 160, at 3 ("In boot camp, recruits are trained to inflict *maximum* damage on enemy personnel.").

161. See, e.g., Banks, *supra* note 160, at 771; Kealy, *supra* note 160, at 386.

162. See WEBER, *supra* note 160, at 10 ("The soldier confronts an enemy in a life-or-death situation" and therefore "learns to use lethal force on the enemy, both uniformed and civilian, irrespective of age or gender."). But see *id.* at 9 (noting that "[i]n the military's newest 'peacekeeping' role abroad, it is obliged—much as civilian police—to be 'highly discreet when applying force'").

163. See, e.g., *Tennessee v. Garner*, 471 U.S. 1, 11 (1985) (declaring unconstitutional a state statute permitting police to use deadly force to apprehend nonviolent fleeing suspects).

164. Mark J. Osiel, *Obedying Orders: Atrocity, Military Discipline, and the Law of War*, 86 CAL. L. REV. 939, 1114 (1998).

165. See Harold J. Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 TEXAS L. REV. 49, 49–50 (1995) (discussing how the Fourth Amendment privacy protections restrain law enforcement activities).

practices—which are entirely justified on the battlefield—from contaminating the separate world of civilian law enforcement with its very different priorities and balancing of equities.

The firewall's benefits run in both directions. Keeping soldiers from enforcing the law doesn't just protect civilians, it also protects the military. If the Armed Forces assume routine law enforcement responsibilities, their scarce resources—financial, equipment, personnel, and otherwise—will be diverted away from their core mission of fighting wars.¹⁶⁶ There is also a more immediate risk that law enforcement responsibilities will blunt the military's combat readiness.¹⁶⁷ In training for and performing police functions, soldiers may begin to acquire some of the institutional cop culture of caution and scrupulous legalism. And that could come at the cost of military effectiveness. “If military personnel are trained to overcome their ‘shoot to kill’ orientation, they may sacrifice their sharpness as soldiers.”¹⁶⁸

The second value served by the Posse Comitatus Act is republicanism. The Act reinforces America's basic commitment to representative self-government and its concomitant aversion to military rule.¹⁶⁹ The founding generation's apprehensions about standing armies are well known and needn't be rehearsed at length here.¹⁷⁰ For John Adams, the Boston Massacre was the inevitable result of the Crown's decision to station Redcoats in the city center and charge them with enforcing civil laws: “[S]oldiers quartered in a populous town, will always occasion two mobs, where they prevent one.—They are wretched conservators of the peace!”¹⁷¹ A more specific formulation of this concern is that the military shouldn't wield any influence in civilian matters; the Supreme Court has averted to the “traditional and strong resistance of Americans to any military intrusion into civilian affairs.”¹⁷² More specific still is the principle that the military should play no role in the enforcement of civil laws.¹⁷³

166. See Kealy, *supra* note 159, at 402–21 (arguing that diversion of military resources can hinder military preparedness).

167. See Banks, *supra* note 159, at 771.

168. *Id.*

169. See *supra* note 150 and accompanying text.

170. See, e.g., Nathan Canestaro, *Homeland Defense: Another Nail in the Coffin for Posse Comitatus*, 12 WASH. U. J.L. & POL'Y 99, 105 (discussing American colonists' view of standing armies as instruments of oppression and tyranny); Dougherty, *supra* note 152, at 4–8 (chronicling the Founders' fear of standing armies); Kealy, *supra* note 159, at 391 (recounting the Founders' arguments against standing armies).

171. John Adams, Argument, in 3 LEGAL PAPERS OF JOHN ADAMS 266 (L. Kinvin Wroth & Hiller B. Zobel eds., 1965).

172. *Laird v. Tatum*, 408 U.S. 1, 15 (1972); see also Banks, *supra* note 159, at 740 (describing the Posse Comitatus Act as “[t]he most concrete manifestation of the American tradition of keeping the military out of domestic civilian affairs”); Scott R. Tkacz, *In Katrina's Wake: Rethinking the Military's Role in Domestic Emergencies*, 15 WM. & MARY BILL RTS. J. 301, 307 (2006) (explaining that Posse Comitatus “reaffirm[s] the deeply held American principle that civilian and military spheres should be kept distinctly separate”). *But see* Felicetti & Luce, *supra* note 150, at 93 (“While the nation's founders were deeply concerned with the abuses of the British Army during

Posse Comitatus helps promote the republican value of self-government by reducing the likelihood that civilian authorities will lose control over the military. The Act excludes the Armed Forces from making even minimal inroads into the world of civilian law enforcement for fear that such a beachhead could eventually cause the military to gain a measure of independence—or even lead to outright military rule. In other words, the Act aims at preventing the nation from taking the first, tentative steps down a slippery slope toward a coup. It’s jarring to read those words. Today, two centuries into the American experiment, with our tradition of civilian control of the military firmly established, the chances that the Armed Forces might take control of the government are vanishingly small, probably even nonexistent.¹⁷⁴ But in 1878, with memories of the Civil War and its attendant military courts, military governors, and other incidents of military rule still fresh, anxieties about the long run viability of republican self-government must have been acute.

The Act helps preserve republicanism in a second, more practical, way. It keeps the military from exerting undue influence in domestic policy debates. The general public—and, derivatively, elected officials—might defer to the Armed Forces because of the stratospherically high esteem in which they are held. In a June 2009 Gallup poll, fully 82% of adults reported having “a great deal” or “quite a lot” of confidence in the military.¹⁷⁵ The military scored 15 points higher than the next most popular choice (small business, weighing in at 67%), and it trounced such also-rans as the presidency (51%), the Supreme Court (39%), and Congress (17%!).¹⁷⁶ It is conceivable that some citizens might embrace the Armed Forces’ policy views, not so much because they independently conclude that those preferences are sound, but because their respect for soldiers is so great that they are simply willing to take the military’s word for it. The Posse Comitatus Act helps prevent that preference substitution by keeping the military from forming (at least some) domestic policy preferences in the first

the colonial period and military interference in civil affairs, the majority was even more concerned about a weak national government incapable of securing life, liberty, and property.” (footnotes omitted)).

173. See Banks, *supra* note 159, at 741 (calling the Posse Comitatus Act “a symbol of our nation’s . . . distaste of military involvement in domestic law enforcement”); Canestaro, *supra* note 171, at 99 (explaining that the Act upholds “a basic value of American democracy—the principle that the military cannot enforce civilian law”); Roger Blake Hohnsbeen, *Fourth Amendment and Posse Comitatus Act Restrictions on Military Involvement in Civil Law Enforcement*, 54 GEO. WASH. L. REV. 404, 404 (1986) (“It is a strong tradition in the United States to eschew the use of military force in the routine enforcement of civil laws.”).

174. See Canestaro, *supra* note 170, at 140 (“The military would rightfully contest any suggestion that their soldiers would either undermine American values or subvert our democracy.”); *id.* at 139 (citing the “dissipation of the fear that Americans have historically harbored towards a standing army”).

175. Lydia Saad, *Americans’ Confidence in Military Up, Banks Down*, GALLUP.COM, June 24, 2009, <http://www.gallup.com/poll/121214/americans-confidence-military-banks-down.aspx>.

176. *Id.*

place.¹⁷⁷ That is, the Act keeps the military from developing an institutional perspective on the law enforcement issues it demarcates as out of bounds. Voters and civilian political leaders thus remain relatively free to deliberate over questions of domestic law enforcement policy without deferring excessively to the military's preferences.

The Posse Comitatus Act gives concrete form to these general principles through a deceptively simple directive:

Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both.¹⁷⁸

That sounds simple enough, but in practice the Act is plagued by ambiguity.¹⁷⁹ Some commentators say the Act bars a fairly wide range of conduct,¹⁸⁰ while others think it doesn't rule out much at all.¹⁸¹ How to construe the Act is of more than academic interest, however, because criminal penalties await those who violate it.¹⁸² No one has ever been prosecuted under the Act,¹⁸³ but uncertainty about its scope and the mere threat of criminal sanctions can deter military officials from taking actions that may well be lawful.

Of particular interest here, it remains unclear to what extent Posse Comitatus allows law enforcement officials and military officers to share information with one another.¹⁸⁴ Indeed, in part because of the Act, military brass appear to be exceedingly reluctant to share information with their

177. See Banks, *supra* note 159, at 740 (describing the Posse Comitatus Act as “[t]he most concrete manifestation of the American tradition of keeping the military out of domestic civilian affairs”).

178. 18 U.S.C. § 1385 (2006).

179. See James Balcius & Bryan A. Liang, *Public Health Law & Military Medical Assets: Legal Issues in Federalizing National Guard Personnel*, 18 ANNALS HEALTH L. 35, 39 (2009) (describing the Act's “brevity and vagueness”); Linda J. Demaine & Brian Rosen, *Process Dangers of Military Involvement in Civil Law Enforcement: Rectifying the Posse Comitatus Act*, 9 N.Y.U. J. LEGIS. & PUB. POL'Y 167, 170 (2005) (explaining that the Act is “riddled with uncertainty and complexity”); Felicetti & Luce, *supra* note 150, at 88 (describing “the confusion surrounding the Posse Comitatus Act”); Tkacz, *supra* note 172, at 309 (arguing that Posse Comitatus “creat[es] uncertainty as to exactly what statutory limits restrict the President in times of emergency”).

180. See, e.g., Felicetti & Luce, *supra* note 150, at 153 (noting that the Department of Defense set forth “an extremely broad interpretation” of the Act—it “prohibits all ‘direct’ DOD participation in law enforcement; civilians should not be subject to military power that is regulatory, proscriptive, or compulsory in nature”).

181. See, e.g., Dougherty, *supra* note 152, at 17–18 (arguing that the Act does not limit the President's use of military as law enforcement under the emergency powers doctrine).

182. 18 U.S.C. § 1385.

183. See Kealy, *supra* note 159, at 405.

184. See Gustav Eyler, *Gangs in the Military*, 118 YALE L.J. 696, 717–19 (2009) (discussing the “military's hesitancy to communicate and cooperate fully with civilian law enforcement agencies” because of cautious interpretations of the Posse Comitatus Act).

colleagues in law enforcement agencies.¹⁸⁵ A series of hypotheticals should help illustrate why.

Imagine that al Qaeda carries out a catastrophic terrorist attack in the United States—say a cell of operatives detonates explosives at a Midwestern shopping mall during the Christmas rush, collapsing the structure and killing hundreds of shoppers. The FBI will play a leading role in the investigation, and it may want to use various military assets. For instance, the Bureau might ask the Pentagon to provide it with overhead imagery of the attack site, either from satellites or from Air Force reconnaissance aircraft; a bird’s-eye view of the blast pattern might reveal some clues about the attack’s origins. Or it might give samples of explosives residue to the Army for forensic analysis; Army experts might be able to shed some light on the type of materiel used in the attack, where it can be obtained, and even the possible identity of the perpetrators. Or the local FBI field commander might ask a counterpart in the U.S. Northern Command for tactical advice on how to most effectively quarantine the attack site and manage access to the rubble.

May the Armed Forces share this sort of information with the FBI? In other words, does it count as “otherwise . . . execut[ing] the laws”¹⁸⁶ within the meaning of the Posse Comitatus Act for the military to give imagery,¹⁸⁷ forensic analysis, and other types of information to a law enforcement agency like the Bureau? The leading federal cases interpreting the Act—a quartet of decisions arising out of the Wounded Knee Siege in the 1970s—send mixed signals.¹⁸⁸

On February 27, 1973, a group of armed men calling themselves the American Indian Movement seized control of Wounded Knee, a town in the southwest corner of South Dakota.¹⁸⁹ Federal law enforcement and military personnel quickly cordoned off the town, and the two sides maintained an uneasy standoff for seventy-one days, sometimes exchanging gunfire.¹⁹⁰ During the siege, the Armed Forces occasionally passed intelligence information to on-site law enforcement officials (mostly imagery taken from reconnaissance planes); they also offered tactical advice, such as tips on how

185. See, e.g., Kealy, *supra* note 159, at 432 (arguing that “the military should not only be allowed, but encouraged, to share information with law enforcement when it is necessary to prevent or investigate criminal activity”).

186. 18 U.S.C. § 1385.

187. Cf. Siobhan Ghorman, *White House to Abandon Spy-Satellite Program*, WSJ.COM, June 23, 2009, <http://online.wsj.com/article/SB124572555214540265.html> (recounting concerns that the Posse Comitatus Act is violated by a program that shares military satellite imagery with domestic agencies).

188. See Canestaro, *supra* note 170, at 127–29 (surveying the contradictory interpretations of the Posse Comitatus Act in the litigation following the Wounded Knee Siege); Felicetti & Luce, *supra* note 150, at 145–46 (discussing the “confusing patchwork of decisions” that resulted from the Wounded Knee Siege); Hohnsbeen, *supra* note 173, at 409–13 (summarizing the holdings in the four seemingly contradictory cases).

189. Canestaro, *supra* note 170, at 126.

190. *Id.* at 126–27.

to end the standoff with a minimum amount of bloodshed.¹⁹¹ A number of the gunmen eventually found themselves in the dock facing a variety of federal criminal charges.¹⁹² The defendants' strategy was to deny that they had committed the crime of interfering with a "law enforcement officer lawfully engaged in the lawful performance of his official duties,"¹⁹³ because the military's involvement at Wounded Knee violated the Posse Comitatus Act and thus rendered the officers' actions unlawful.¹⁹⁴

Two judges agreed. *United States v. Jaramillo*¹⁹⁵ held that the soldiers had so "perva[sively]" assisted the cops that there was a reasonable doubt whether the latter were lawfully engaged in the lawful performance of their duties.¹⁹⁶ One of the things the *Jaramillo* court cited as an example of impermissible military involvement was giving tactical advice to law enforcement officials—a form of information sharing.¹⁹⁷ Similarly, in *United States v. Banks*,¹⁹⁸ the court found that the totality of the evidence suggested that the military's involvement at Wounded Knee crossed the line into a Posse Comitatus violation (though it did not identify specific acts that offended the statute).¹⁹⁹ Two other judges saw things differently. *United States v. Red Feather*²⁰⁰ held that only the "direct active use" of soldiers to enforce the law violates the Posse Comitatus Act.²⁰¹ Anything short of that—including the military's behind-the-scenes assistance at Wounded Knee—is permissible. Likewise, *United States v. McArthur*²⁰² held that the information sharing and other forms of assistance did not offend the Posse Comitatus Act, because the Armed Forces did not subject citizens to military power that was "regulatory, proscriptive, or compulsory."²⁰³

Given these precedents, may the military share satellite imagery, forensics analysis, tactical advice, and other types of information with the FBI in the wake of a domestic terrorist attack? Under *Jaramillo* and *Banks*, that may well violate Posse Comitatus.²⁰⁴ Under *Red Feather* and *McArthur*,

191. Hohnsbeen, *supra* note 173, at 409.

192. *Id.* at 409–10.

193. 18 U.S.C. § 231(a)(3) (2006).

194. Canestaro, *supra* note 170, at 127.

195. 380 F. Supp. 1375 (D. Neb. 1974).

196. *Id.* at 1379–81.

197. *Id.* at 1381.

198. 383 F. Supp. 368 (D.S.D. 1974).

199. *See id.* at 375–76 (holding that the evidence did not support a conclusion that the government activity was lawful).

200. 392 F. Supp. 916 (D.S.D. 1975).

201. *See id.* at 923 (discussing the broad authority granted to the military to involve itself indirectly with civilian law enforcement operations).

202. 419 F. Supp. 186 (D.N.D. 1976), *aff'd sub nom.* *United States v. Casper*, 541 F.2d 1275 (8th Cir. 1976).

203. *Id.* at 194–95.

204. *See Banks*, 383 F. Supp. at 375–76 (citing the use of military equipment and tactical consultation with military personnel as an example of conduct that may be impermissible under the

it probably doesn't.²⁰⁵ That uncertainty may be enough to keep the Armed Forces from swapping data with the Bureau; risk-averse officials may decide that the safest bet is to avoid any conduct that even arguably violates the act—especially since a Posse Comitatus violation is a crime that could land one in jail.²⁰⁶

Of course, Congress is free to carve out exceptions to Posse Comitatus, and it has done so on a number of occasions.²⁰⁷ The legality of information sharing is complicated by a 1981 exception intended to promote military cooperation with criminal investigations of narcotics trafficking in the Caribbean;²⁰⁸ it provides that “[t]he Secretary of Defense may . . . provide . . . civilian law enforcement officials any information collected during the normal course of military training or operations.”²⁰⁹ The idea seems to be that the Armed Forces may share intelligence with law enforcement if they just so happen to come across it in the ordinary course of business, but they may not—and this is key—share intelligence they have deliberately set out to collect on law enforcement’s behalf.²¹⁰ The 1981 amendment thus reflects something like the “plain view” doctrine from Fourth Amendment law.²¹¹ Let’s return to our hypothetical attack. It’s unclear whether overhead imagery, forensic analysis, and other intelligence provided by the Armed Forces to the FBI would count as “collected during the normal course of military training or operations.”²¹² In this scenario, as is likely to be the case in the real world, the military is actively partnering with law enforcement. The cops are not mere passive recipients of whatever the military chooses to

Posse Comitatus Act); *United States v. Jaramillo*, 380 F. Supp. 1375, 1381 (D. Neb. 1974) (citing the provision of military advice and information as examples of conduct that may be impermissible under the Posse Comitatus Act).

205. See *McArthur*, 419 F. Supp. at 194 (explaining that a violation of the Posse Comitatus Act requires military action that is “regulatory, proscriptive, or compulsory,” which would be beyond mere intelligence sharing); *Red Feather*, 392 F. Supp. at 923 (holding that only “direct active use” of soldiers to enforce the law violates the Posse Comitatus Act).

206. See *supra* note 75 and accompanying text.

207. See, e.g., 10 U.S.C. § 332 (2006) (authorizing the President to use the Armed Forces to put down “unlawful obstructions, combinations, or assemblages, or rebellion against the authority of the United States,” when it is “impracticable to enforce the laws of the United States in any state by the ordinary course of judicial proceedings”).

208. See Hohnsbeen, *supra* note 173, at 416–19.

209. 10 U.S.C. § 371(a) (2006).

210. For instance, the House Report discussing the 1981 amendment suggests that “the scheduling of routine training missions can easily accommodate the need for improved intelligence information concerning drug trafficking in the Caribbean.” H.R. REP. NO. 97-71, pt.2, at 8 (1981); see also Hohnsbeen, *supra* note 173, at 422 (speculating that “the military could alter its normal course of operations to accommodate civilian needs”). In practical terms, this would mean that the Air Force may not fly reconnaissance missions whose express purpose is to surveil offshore drug smugglers. But it would be permissible to inform the cops if a routine training flight happens to find evidence of narcotics trafficking. And it would be permissible to schedule routine training flights in the hopes that such evidence will be uncovered.

211. See, e.g., *Arizona v. Hicks*, 480 U.S. 321 (1987).

212. 10 U.S.C. § 371(a).

send them; they are collaborating to ensure that military collection meets the FBI's needs. That active role for law enforcement in determining the Armed Forces' intelligence activities may remove the resulting intelligence take from the murky category of "normal . . . military operations"²¹³ and place it squarely in the realm of "otherwise . . . execut[ing] the laws."²¹⁴

Even more vexing line-drawing problems can arise. Consider the complications that result from the fact that the FBI is a hybrid entity that combines both law enforcement responsibilities and domestic intelligence functions.²¹⁵ Roughly speaking, the Bureau has two options for how to handle our hypothetical mall bombing: through a criminal investigation or an intelligence investigation.²¹⁶ Which tack the FBI takes could make a big difference to the Posse Comitatus analysis. If the Armed Forces share information with Bureau personnel who are treating the attack primarily as an intelligence matter, the Act's strictures may not be implicated.²¹⁷ But what if the military shares the very same information with the very same FBI personnel when the latter are engaged in a criminal investigation? That may well count as "execut[ing] the laws";²¹⁸ the Armed Forces would be gathering information, probably at the FBI's direction, that is specifically intended to be used as evidence in subsequent criminal proceedings. Military officers thus could find themselves criminally liable under the Posse Comitatus Act because of how the FBI chooses to use the information it receives. Perversely, what would trigger liability would not be the military's own actions, but the actions of the recipient agency.

Even worse, the character of the FBI's investigation may not be readily apparent, and it may even change over time; retroactivity problems can occur here, too.²¹⁹ In the immediate aftermath of the attack, it is unlikely that the Bureau will have decided whether to put the matter on the criminal track or the intelligence track.²²⁰ It will want to keep its options open. Indeed, one of the principal aims of the early stages of the investigation will be to learn enough about the attack to decide whether it warrants treatment as a garden-

213. *Id.*

214. 18 U.S.C. § 1385 (2006).

215. See POSNER, *supra* note 24, at 101 (referencing the "marriage of criminal investigation and domestic intelligence in the FBI").

216. OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FBI'S HANDLING OF INTELLIGENCE INFORMATION PRIOR TO THE SEPTEMBER 11 ATTACKS 10 (2005) [hereinafter FBI REPORT] ("International terrorism could be investigated as both an intelligence and as a criminal investigation.").

217. See JAMES P. HARVEY, NOT IN OUR OWN BACKYARD: POSSE COMITATUS AND THE CHALLENGE OF GOVERNMENT REORGANIZATION 16–17 (2008) (describing an example of the Department of Defense sharing information with the FBI after the latter launched an intelligence investigation of the 1996 Khobar Towers attack).

218. 18 U.S.C. § 1385.

219. See *supra* note 140 and accompanying text.

220. See FBI REPORT, *supra* note 216, at 19–20 (describing the different procedures and requirements for opening criminal and intelligence investigations).

variety crime or whether it is significant enough to be treated as an intelligence matter. This is the stage of the investigation when the military's assets will prove most helpful to the FBI. But it's also the stage when the investigation's character—is it criminal or is it intelligence?—is most difficult to pin down. That ambiguity encourages the Armed Forces to sit on the sidelines just when their resources are needed the most. Why take a chance and risk two years in jail? Now suppose the FBI initially decides to treat the attack as an intelligence matter, but after receiving information from the military it changes course and opens a criminal investigation. At the time the sharing took place, it had no connection to a law enforcement investigation and thus was lawful under the Posse Comitatus Act. Now? It's hard to say. Sharing that was once lawful could become retroactively unlawful, due to the Bureau's about-face. (The Constitution's *ex post facto* clause presumably would bar the retroactive imposition of criminal liability for data exchange that was lawful at the time it took place.²²¹)

Up to this point we have only considered data flowing in one direction—from the Armed Forces to law enforcement. What about sharing in the opposite direction? Might the Posse Comitatus Act restrict the FBI from sharing data collected in the course of a criminal investigation with the military? Suppose prosecutors discover through grand jury testimony that the mall bombing was carried out by an al Qaeda cell that trained at a previously unknown camp in Yemen. May they alert the military in the hopes that the Armed Forces will raze the camp?

This sort of transaction is not covered by the 1981 amendment. That exception only authorizes sharing from soldiers to cops; it is silent on sharing from cops to soldiers. “The *Secretary of Defense* may . . . provide . . . *civilian law enforcement officials* any information collected during the normal course of military training or operations.”²²² The 1981 legislation thus may have something like an *expressio unius* effect, ruling out data exchange between the military and law enforcement that is not specifically authorized.²²³ Congress's decision to allow certain kinds of sharing implies a deliberate decision to preclude all other kinds. The question then becomes whether, in Posse Comitatus terms, the Armed Forces “execute the laws” when they use in military operations data that was gathered for law enforcement reasons. Information that originally was collected for law

221. U.S. CONST. art. I, § 9, cl. 4.

222. 10 U.S.C. § 371(a) (2006) (emphasis added).

223. See 2A NORMAN J. SINGER & J.D. SHAMBIE SINGER, SUTHERLAND STATUTORY CONSTRUCTION § 47:23 (7th ed. 2007). According to the Singer treatise,

As the maxim [*expressio unius est exclusio alterius* (the expression of one is the exclusion of others)] is applied to statutory interpretation, where a form of conduct, the manner of its performance and operation, and the persons and things to which it refers are designated, there is an inference that all omissions should be understood as exclusions.

Id.

enforcement conceivably might retain that character even when passed on to different government officials who mean to use it for different (though related) purposes. This kind of exchange isn't obviously unlawful, but it doesn't have to be. For a government official looking at a two-year jail term, legal uncertainty may be enough to deter information sharing.²²⁴

Privacy Act

Most commentators agree that the Privacy Act of 1974 doesn't impose meaningful limits on the ability of intelligence agencies to share information with one another.²²⁵ While the Act sweepingly bars officials from disclosing covered records without the data subject's consent,²²⁶ it is riddled with loopholes that give agencies fairly wide latitude to exchange data.²²⁷ Or so the story goes. I will argue that, in reality, the Privacy Act's exemptions are not as gaping as is commonly supposed, and the Act—especially its requirement that any “routine” disclosure of data from one agency to another must be “compatible” with the purpose for which it originally was collected²²⁸—could saddle officials with serious sharing restrictions.

At the risk of stating the obvious, the Privacy Act promotes *individual privacy*. The statute vindicates both aspects of privacy discussed above—privacy as freedom from the government observing personal facts about oneself, and privacy as the ability autonomously to control the manner in which one's information is presented to others.²²⁹ The Privacy Act—Congress's first systematic effort to protect the privacy of personal information against government intrusions—was passed because of anxiety about fast-moving technological developments.²³⁰ Computer-based systems were being deployed, both in government and in the private sector, that were capable of storing, indexing, and retrieving previously unimaginable troves of data, and Congress grew increasingly worried about the baleful consequences of these new technologies for individual privacy.²³¹

224. See *supra* note 75 and accompanying text.

225. See Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. REV. 609, 694–97 (2007) (arguing that the Privacy Act should be amended to better protect information privacy, including by eliminating “[f]ree-for-all information sharing”); see also Fred H. Cate, *Governing Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 465–66 (2008) (describing the numerous broad exceptions in the Privacy Act).

226. 5 U.S.C. § 552a(b) (2006).

227. Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 379.

228. 5 U.S.C. § 552a(7).

229. See *supra* notes 65–71 and accompanying text.

230. See Privacy Act of 1974, Pub. L. No. 93-579, § 2(a), 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a (2006)) (“[T]he increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information.”).

231. See, e.g., S. REP. NO. 93-1183, at 15 (1974) (“[T]he creation of formal or de facto national data banks, or of centralized Federal information systems without certain statutory guarantees

The Privacy Act addresses that concern in a number of concrete ways.²³² Its most significant feature is its sweeping requirement that “[n]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.”²³³ Congress saw this nondisclosure requirement as “one of the most important, if not the most important, of the bill.”²³⁴ The Act contains a number of exceptions to its general prohibition on unconsented sharing of personal data.²³⁵ By far the most important is the exemption that allows records to be shared for a “routine use.”²³⁶ Under this provision, an agency is allowed to disclose a covered record to other officials if two hurdles are cleared. First, the “use of such record [must be] for a purpose which is compatible with the purpose for which it was collected”;²³⁷ second, the agency must publish a notice in the Federal Register.²³⁸

The conventional wisdom is that, thanks to these and other loopholes, the Act does an exceptionally poor job of protecting individual privacy. The Act has been described as “less protective of privacy than may first appear”²³⁹ and “weak and ineffectual by today’s standards.”²⁴⁰ And those are the favorable reviews. Others say the Privacy Act is either “a paper tiger,”²⁴¹ or “purely hortatory” and “entirely ineffective,”²⁴² or little more than “a procedural notice statute, rather than a safeguard against government invasion of individual privacy.”²⁴³ There is also widespread agreement that the Act doesn’t prevent intelligence agencies from swapping data. The Markle Foundation’s Task Force on National Security in the Information Age confidently predicted that “future government initiatives promoting increased interagency information sharing to protect national security will

would . . . threaten . . . the values of privacy and confidentiality in the administrative process.”); James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 35 (2003) (citing “the rapid development in record-keeping systems in both government and the private sector,” as well as “the computerization of information storage, retrieval, and data processing,” as influencing Congress’s decision to enact the Privacy Act).

232. See, e.g., 5 U.S.C. § 552a(e)(5) (directing agencies to maintain their records accurately); *id.* § 552a(d) (guaranteeing persons the right to inspect any records pertaining to them and to correct any inaccurate information).

233. *Id.* § 552a(b).

234. H.R. REP. NO. 93-1416, at 12 (1974); see also, e.g., BeVier, *supra* note 69, at 479 (describing the nondisclosure requirement as “the heart of the Privacy Act”).

235. See *supra* note 227 and accompanying text.

236. 5 U.S.C. § 552a(b)(3).

237. *Id.* § 552a(a)(7).

238. *Id.* § 552a(e)(4)(D).

239. Cate, *supra* note 225, at 465.

240. Nehf, *supra* note 231, at 40.

241. BeVier, *supra* note 69, at 479.

242. Bignami, *supra* note 225, at 633.

243. Todd Robert Coles, *Does the Privacy Act of 1974 Protect Your Right to Privacy? An Examination of the Routine Use Exemption*, 40 AM. U. L. REV. 957, 979 (1991).

meet with little resistance” from the Privacy Act.²⁴⁴ Academic commentators agree. “Certainly,” one article intones, “this allows all agencies involved in counterterrorism to share information.”²⁴⁵

The Privacy Act’s exemptions may be fairly broad, but they do not give agencies anything like *carte blanche* to exchange intelligence with one another. Even the much maligned routine use exemption may prohibit a great deal of information sharing. To be sure, some courts interpret the compatibility requirement fairly weakly. But others courts regard compatibility as a significant hurdle.²⁴⁶ Routine use could prove a meaningful constraint on data exchange under this latter approach.

The most restrictive readings come from the Third and Ninth Circuits. In *Britt v. Naval Investigative Service*,²⁴⁷ the defendant agency disclosed information about a Marine Corps reservist to his employer, the Immigration and Naturalization Service (INS); Britt was the subject of a criminal investigation and the NIS believed the INS “might find it relevant to have information suggesting [his] lack of integrity.”²⁴⁸ The court found the disclosure impermissible, holding that mere “[r]elevance” does not satisfy the routine use exemption’s compatibility requirement.²⁴⁹ “Congress limited interagency disclosures to more restrictive circumstances,” it explained.²⁵⁰ “There must be a more concrete relationship or similarity, some meaningful degree of convergence, between the disclosing agency’s purpose in gathering the information and in its disclosure.”²⁵¹ Under the Third Circuit’s approach, records that one agency gathers for law enforcement purposes may not be shared with another agency even if they concededly would be relevant to the latter’s mission. The Ninth Circuit took a similar tack in *Swenson v. U.S.*

244. MARKLE FOUND., PROTECTING AMERICA’S FREEDOM IN THE INFORMATION AGE 130 (2002).

245. Dempsey & Flint, *supra* note 70, at 1475; *see also* BeVier, *supra* note 69, at 477 (arguing that the Act “place[s] relatively few substantive barriers in the way of inter- or intra-governmental sharing of personal information”); Bignami, *supra* note 69, at 672 (arguing that agency use of intelligence information is “almost entirely unregulated” by the Act).

246. *See* MARKLE FOUND., *supra* note 244, at 129–30 (indicating that at least one court has interpreted the compatibility requirement strictly, requiring the showing of a meaningful nexus before the compatibility exception can be satisfied); Coles, *supra* note 243, at 999 (“Judicial enforcement of the . . . compatibility test[] has successfully prevented some abuses of the routine use exemption by federal agencies.”); *cf.* BeVier, *supra* note 69, at 482–84 (noting that because the statute does not “prescribe a standard of compatibility,” government agencies are free to interpret the provision narrowly or quite broadly and that the broad interpretations of the provision are the most worrisome); Cate, *supra* note 225, at 465 (“According to the Office of Management and Budget, ‘compatibility’ covers uses that are either (1) functionally equivalent or (2) necessary and proper.”).

247. 886 F.2d 544 (3d Cir. 1989).

248. *Id.* at 549.

249. *Id.*

250. *Id.*

251. *Id.* at 549–50.

Postal Service.²⁵² The plaintiff, a mail carrier in California, wrote letters to a senator and congressman alleging that her postmaster was deliberately undercounting rural mail routes.²⁵³ In response to inquiries from those officeholders, the Postal Service revealed that the plaintiff had filed a sex discrimination complaint with the EEOC.²⁵⁴ The court ruled that the disclosure (the purpose of which was to respond to a congressional inquiry) was not compatible with the purpose for which the information was collected (namely, “to adjudicate complaints of alleged discrimination and to evaluate the effectiveness of the EEO program”).²⁵⁵ Citing the Third Circuit’s ruling in *Britt*, the court emphasized that “compatibility requires more than mere relevance.”²⁵⁶

The D.C. Circuit takes a more flexible view of routine use. In *U.S. Postal Service v. National Association of Letter Carriers*,²⁵⁷ the court held that the compatibility requirement did not bar the Postal Service from complying with an arbitration award directing it to turn over employee information to the union.²⁵⁸ The court reasoned that, “in common usage, the word ‘compatible’ means simply ‘capable of existing together without

252. 890 F.2d 1075 (9th Cir. 1989).

253. *Id.* at 1076.

254. *Id.*

255. *Id.* at 1078 (quoting 47 Fed. Reg. 1203 (Jan. 11, 1982)).

256. *Id.*; *cf.* *Covert v. Harrington*, 876 F.2d 751, 755 (9th Cir. 1989) (remarking that collection of data for security clearance purposes would not be compatible with disclosure in connection with a criminal investigation). There are some indications that Congress preferred a restrictive understanding of the compatibility requirement. *See* Coles, *supra* note 243, at 971, 976 (explaining that, although the House Bill’s routine use exemption reflected an incremental approach to safeguarding individual privacy in personal information, the House Committee recognized the potential for abuse and therefore “pledged to oversee vigorously federal agency use of the exemption”). The House version of the bill would have allowed agencies to disclose records pursuant to a routine use; the Senate rejected such an exemption for fear that agencies would abuse it. *Id.* at 976. The compromise was to retain the House’s routine use exemption while adding the compatibility requirement to limit agency discretion to transfer information. *Id.* at 978 (“While the House bill permitted the federal agency discretion when establishing routine uses, the compromise language required that the routine use be compatible with the purpose for which information was collected.”). Later, various members of Congress would reiterate their understanding that the compatibility requirement had some bite. *See, e.g.*, H.R. REP. NO. 101-927, at 67 (1990). The Report notes:

Agencies proceed on the apparent belief that any disclosure can be authorized as long as a routine use has been established in accordance with the Privacy Act’s procedures. This is a distortion of the law. There must be a connection between the purpose of the disclosure and the purpose for which the information was collected. In the absence of a sufficient nexus between these two purposes, an agency cannot create routine uses simply because a disclosure would be convenient or to avoid the procedural requirements established in [the nondisclosure provision] of the Privacy Act.

Id.

257. 9 F.3d 138 (D.C. Cir. 1993).

258. *Id.* at 145–46.

discord or disharmony.”²⁵⁹ It therefore concluded that disclosures are only impermissible if they would undermine the agency’s reasons for collecting the data in the first place.²⁶⁰ “[S]o long as a proposed disclosure would not actually frustrate the purposes for which the information was gathered, [the compatibility] requirement would be met. Only in rare cases would disclosure run afoul of such a dictate.”²⁶¹ The court went on specifically to reject the Third Circuit’s reasoning in *Britt*, partly because such a restrictive understanding “would forbid an agency from disclosing information pursuant to a routine use unless its purpose in disclosure would be virtually identical to its purpose in gathering the information in the first place.”²⁶² For the D.C. Circuit, routine use isn’t much of a limit on interagency information sharing.²⁶³

Many types of information sharing would be impermissible under the Third and Ninth Circuits’ strict reading of compatibility. Consider two examples. First, U.S. Customs and Border Protection collects basic information about container ships transporting goods to the United States—e.g., the names of the crew, previous ports of call, the owners of the vessels, the owners of the cargo, and so on.²⁶⁴ The agency uses this data to identify vessels that might be carrying contraband, such as illegal narcotics or counterfeit goods that infringe various intellectual property rights.²⁶⁵

259. *Id.* at 144 (quoting WEBSTER’S THIRD NEW INTERNATIONAL DICTIONARY 463 (2d ed. 1971)).

260. *Id.*

261. *Id.*

262. *Id.* at 145.

263. The Office of Management and Budget—the agency that administers the Privacy Act—apparently has cast its lot with the D.C. Circuit’s permissive approach. According to OMB, a disclosure satisfies the compatibility requirement if the recipient agency’s intended use is either “functionally equivalent” or “necessary and proper” to the sharing agency’s use. Privacy Act of 1974; Guidance on the Privacy Act Implications of “Call Detail” Programs to Manage Employees’ Use of the Government’s Telecommunications Systems, 52 Fed. Reg. 12,990, 12,993 (Apr. 20, 1987). If “necessary and proper” in the Privacy Act context means something similar to what it famously means in the Constitution, it should be fairly easy to establish compatibility. See *McCulloch v. Maryland*, 17 U.S. (4 Wheat.) 316, 421 (1819) (holding that, if the end is “legitimate,” then “all means which are appropriate, which are plainly adapted to that end, [and] which are not prohibited” are “necessary and proper” within the meaning of the Constitution). Because OMB is charged by Congress with administering the Privacy Act, its interpretation of the scope of the compatibility requirement may be entitled to judicial deference under the *Chevron* doctrine. See *Chevron U.S.A., Inc. v. Natural Res. Def. Council, Inc.*, 467 U.S. 837, 844 (1984) (holding that explicit gaps in delegations of statutory authority to administrative agencies are to be construed as express delegations of authority to interpret by regulation, given controlling weight by the courts unless arbitrary, capricious, or manifestly contrary to statute).

264. See U.S. CUSTOMS AND BORDER PROTECTION, CBP FORM 1302, INWARD CARGO DECLARATION (2009), available at http://forms.cbp.gov/pdf/CBP_Form_1302.pdf (collecting previous port, vessel owner, and cargo owner information); U.S. CUSTOMS AND BORDER PROTECTION, CBP FORM I-418, PASSENGER LIST—CREW LIST (2009), available at http://forms.cbp.gov/pdf/CBP_Form_I418.pdf (collecting crew and previous port information).

265. See Press Release, U.S. Customs and Border Protection, CBP Officers Seized More Than \$5 Million in Narcotics and Currency at Laredo Port of Entry (Mar. 8, 2010), available at

Suppose Customs wants to hand over its records to the NSA. It reasons that, if analyzing vessel data is a good way to detect contraband, it may also be a good way to detect al Qaeda operatives trying to sneak into the country. And Customs knows that the NSA's analytical capabilities are more advanced than its own. Would NSA's use of the records for counterterrorism purposes be compatible with the purposes for which Customs originally compiled them—namely, to detect knockoff Jackie Chan DVDs and Mickey Mouse dolls stuffed with heroin? A court following *Britt* might conclude that there's a fundamental difference between using data to screen for contraband and using data to screen for suspected terrorists; there's no "concrete relationship," "similarity," or "meaningful degree of convergence" between screening for goods and screening for people;²⁶⁶ the two purposes aren't "virtually identical."²⁶⁷

Second, the Environmental Protection Agency collects information about factories and other sources of air pollution, such as the names of facility owners, contact information for managers, and emissions levels. It does so to enforce the Clean Air Act—e.g., to determine whether regulated entities are emitting pollutants without the requisite permits, to assess whether a given source's emissions exceed its permitted allotment, and so on.²⁶⁸ Suppose the EPA wants to share its records with Homeland Security. DHS thinks the data will come in handy for a number of its counterterrorism responsibilities—to help assess the vulnerability of the nation's critical infrastructure to terrorist attacks, to determine the likely consequences for the surrounding areas of a terrorist attack on a plant, and to inform its decisions about which parts of the country should receive preparedness grants. Would DHS's terrorism-related use of the records be compatible with the EPA's enforcement-related reasons for collecting them in the first place? Again, the answer is far from obvious. A court may reason that there is no nexus between using factory data to limit the amount of sulfur dioxide released into the atmosphere, on the one hand, and using it to prevent terrorist attacks, on the other.

Agencies may be especially reluctant to push the information sharing envelope because of the sanctions that can be imposed for disclosing records

http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/march_2010/03082010_2.xml (providing an example of narcotics seizures resulting from Customs's searches of shipping at a port of entry); Press Release, U.S. Customs and Border Protection, Miami CBP Seizes Counterfeit Designer Merchandise Valued at \$5.2 Million (Mar. 24, 2010), available at http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/march_2010/03242010_2.xml (providing an example of counterfeit-good seizure resulting from Customs's searches of shipping at a port of entry).

266. *Britt v. Naval Intelligence Serv.*, 886 F.2d 544, 549–50 (3d Cir. 1989).

267. *U.S. Postal Serv. v. Nat'l Ass'n of Letter Carriers*, 9 F.3d 138, 145 (D.C. Cir. 1993).

268. United States Environmental Protection Agency, Facilities and Enforcement Activities Related to the Clean Air Act Stationary Source Program (Dec. 22, 2009), <http://www.epa.gov/compliance/data/results/performance/caa/>.

in violation of the Privacy Act.²⁶⁹ The Act generally does not authorize penalties, criminal or otherwise, against individual officers who violate its terms.²⁷⁰ But it does allow a person injured by an unlawful disclosure to bring a civil action for money damages against the offending agency.²⁷¹ To be sure, the penalties are fairly modest. An offending agency is only on the hook for the “actual damages” sustained,²⁷² not punitive damages or any resulting emotional damages²⁷³—a far cry from the prospect of jail time under the Posse Comitatus Act.²⁷⁴ Even so, the existence of penalties, however slight, for unlawful disclosures may be enough to deter intelligence agencies from exchanging data they otherwise would have been willing to share.²⁷⁵

Recalibrating the Law and Policy of Information Sharing

Is it possible to expand information sharing without doing violence to pretext, firewall, republicanism, and privacy values? And is it possible to preserve those principles without unduly restricting information sharing? In general, the answer to both questions is yes. Congress had good reasons to enact the National Security Act, the Posse Comitatus Act, and the Privacy Act. But the laws are overbroad; they extend beyond the harmful conduct Congress sought to prohibit and have the potential to restrict desirable information sharing. My analysis of how to accommodate these competing concerns is informed by rational choice theory—the notion that government officials act to maximize their respective interests.²⁷⁶ Looking beyond the

269. See, e.g., 5 U.S.C. § 552a(g) (2006) (allowing for civil suits against the offending agency); *id.* § 552a(i) (providing for criminal penalties against certain offending employees of government agencies).

270. The Privacy Act imposes criminal sanctions in a narrow set of circumstances. An official is guilty of a misdemeanor and faces up to a \$5,000 fine if he “willfully discloses” covered material “knowing that disclosure of the specific material is so prohibited” by law. *Id.* § 552a(i)(1) (emphasis added). The Act thus only punishes officials who share information despite their personal knowledge that the law prohibits it from being disclosed. If officials are merely uncertain whether a disclosure is unlawful, the Privacy Act’s criminal penalties apparently do not apply.

271. See *id.* § 552a(g)(1) (allowing for civil suits against the offending agency); *id.* § 552a(g)(4) (specifying the monetary damages allowable in civil actions under the Privacy Act).

272. *Id.* § 552a(g)(4)(A).

273. See *Doe v. Chao*, 540 U.S. 614, 617–18 (2004) (holding that uncorroborated emotional distress is not sufficient proof of “actual damages” for the purpose of claiming recovery under the Privacy Act); *Fitzpatrick v. IRS*, 665 F.2d 327, 330 (11th Cir. 1982) (noting that the legislative history of the Privacy Act indicates a congressional intent to exclude punitive damages from “actual damages”). *But see* *Cooper v. Fed. Aviation Admin.*, 596 F.3d 538, 540 (9th Cir. 2010) (holding that nonpecuniary damages for humiliation, mental anguish, and emotional distress constitute “actual damages” under the Privacy Act).

274. 67 U.S.C. § 1385 (2006).

275. See *supra* note 75 and accompanying text.

276. See, e.g., AMY B. ZEGART, *SPYING BLIND* 1–14 (2007) (using public choice and organizational theory principles to explain intelligence failures that culminated in 9/11); see also O’Connell, *supra* note 35, at 1679–80 (using public choice and organizational theory principles to explain reorganization of intelligence agencies); Sales, *supra* note 13, at 304–13 (using public choice principles to explain intelligence agencies’ reluctance to share information). See generally WILLIAM A. NISKANEN, JR., *BUREAUCRACY AND REPRESENTATIVE GOVERNMENT* (1971)

text of the law enables us to weigh the effects that various legal requirements have on incentives within military, intelligence, and law enforcement agencies. Harnessing these incentives can help reconcile the goods of information sharing, privacy, republicanism, and the like, in ways that the blunt instrument of the law by itself cannot.

As I will argue, it is unlikely that the CIA and the FBI will collaborate on pretextual surveillance. The CIA will have strong incentives to decline requests by its bureaucratic rival to collect evidence for use in criminal proceedings because doing so would harm the CIA's own interests.²⁷⁷ Similarly, sharing probably won't raise firewall concerns under the 1947 Act or the Posse Comitatus Act;²⁷⁸ data exchange can actually vindicate firewall values by mitigating agencies' incentives to use aggressive intelligence and military techniques in inappropriate spheres.²⁷⁹ Republicanism concerns—the notion that the Armed Forces must always be subordinate to civilian authorities—don't justify sharing restrictions; the potential harms are either too unlikely to materialize or too slight.²⁸⁰ Finally, information sharing may preserve privacy values more effectively than a categorical bar on data exchange; sharing can reduce agencies' incentives to engage in duplicative rounds of privacy-eroding surveillance.²⁸¹ Congress therefore should amend the National Security Act, the Posse Comitatus Act, and the Privacy Act to clearly authorize intelligence and military officials to share counterterrorism information with one another. It isn't necessary to wipe these laws from the statute books altogether; indeed, it would be inadvisable to do so. Instead, Congress should retain each Act's core prohibitions while clarifying that these restrictions don't stand in the way of data exchange.

Pretext Concerns

Like FISA, the National Security Act of 1947—which prohibits the CIA from exercising any “police, subpoena, or law enforcement powers” or performing any “internal security functions”²⁸²—embodies pretext concerns. The Act tries to keep law enforcement officers from commissioning CIA officials (whether explicitly or, more likely, with a wink and a nudge) to collect the evidence they seek under the comparatively relaxed legal standards that apply to intelligence operations.²⁸³ Maintaining the legal limits on domestic surveillance is a worthwhile goal, but the risk that the FBI will task the CIA with pretextual surveillance seems fairly low. The CIA will have strong incentives to resist the Bureau's efforts to goad it into

(developing a public choice account of administrative agency action); JAMES Q. WILSON, BUREAUCRACY (2d ed. 2000) (same).

277. See *infra* notes 284–95 and accompanying text.

278. See *infra* subpart III(B).

279. See *infra* subpart III(B).

280. See *infra* subpart III(C).

281. See *infra* subpart III(D).

282. 50 U.S.C. § 403-4a(d)(1) (2006).

283. See *supra* notes 122–33 and accompanying text.

collecting evidence for use in criminal proceedings; Agency officials will fear that engaging in surveillance on behalf of their rival will enhance the FBI's welfare at the expense of their own.²⁸⁴ The CIA is likely to decline the Bureau's invitations for a more immediate reason as well: such surveillance runs afoul of the 1947 Act.²⁸⁵ In short, it isn't necessary to restrict data exchange between the FBI and the CIA in an effort to prevent improper tasking, because the CIA's pursuit of its institutional interests typically will accomplish the same result.

Information sharing might allow intelligence and law enforcement agencies to collaborate in ways that enable the latter to avoid some of the legal limits on their ability to collect evidence in criminal investigations. The problem is that it can be difficult to determine the precise reasons why two agencies are swapping data with one another. A sharing arrangement between the FBI and the CIA might be completely above board; the two may be running a joint operation in which the CIA conducts surveillance overseas, the FBI conducts surveillance at home, and the resulting intercepts are exchanged throughout both agencies. Or such sharing might strike at the heart of the pretext concerns embodied in the 1947 Act; the FBI may have commissioned the CIA to act as its evidence-gathering surrogate with the latter now dutifully reporting what it has found. From the standpoint of an outside observer, it will not always be apparent whether a given sharing arrangement is innocuous or sinister. It's an evidentiary problem; data exchange that raises pretext problems will look quite similar to data exchange that is entirely innocent.

Still, an information sharing wall between the FBI and the CIA is unnecessary because the two are unlikely to collaborate on pretextual surveillance. The Agency and the Bureau have spent decades waging a fierce turf war,²⁸⁶ and the CIA won't be eager to come to the aid of its interagency rival. Part of the explanation for this intense rivalry is that CIA spies and FBI cops produce competing "goods"—the agencies represent two radically different options for how to deal with national security threats.²⁸⁷ Generally speaking, criminal investigators at the FBI will want to use the standard tools of criminal law to neutralize a given terrorist—indict him for the crimes he has committed, try him, convict him, and incarcerate (or execute) him.²⁸⁸ CIA officials will want to treat the terrorist as an intelligence asset—question him to find out if he knows about plans to strike

284. See Sales, *supra* note 13, at 282–83 (arguing that intelligence agencies hoard information to ward off competition from bureaucratic rivals).

285. See 50 U.S.C. § 403-4a(d)(1) (providing that the CIA Director "shall have no police, subpoena, or law enforcement powers or internal security functions").

286. See generally MARK RIEBLING, WEDGE: FROM PEARL HARBOR TO 9/11 (2002) (chronicling sixty years of interagency conflict in connection with incidents that range from Watergate to the Aldrich Ames spy case).

287. See POSNER, *supra* note 1, at 29–31, 173–82.

288. *Id.* at 173.

the United States, try to turn him into a double agent who can be used to feed misinformation back to al Qaeda, and so on.²⁸⁹

This rivalry will give the CIA powerful incentives not to assist FBI criminal investigations, because doing so could benefit the Bureau's interests at the expense of its own. Even in a case where the target is an ordinary criminal—i.e., a person whose conduct is not remotely related to national security concerns—the CIA will be reluctant to collect evidence for FBI criminal purposes because that would enhance the welfare of its primary bureaucratic competitor. That is, helping the FBI to conduct a criminal investigation will bolster the Bureau's influence (its ability to persuade senior executive branch policy makers, such as the President, to accept its recommendations), as well as its autonomy (its ability to achieve its priorities without interference by outside entities).²⁹⁰ The President and the Attorney General will be marginally more likely in the future to credit the Bureau's recommendations that, say, a particular mob boss should be indicted, or that a particular terrorist should be dealt with through the criminal justice system rather than military commissions. Such topcover from senior officials also will make the FBI marginally more effective at shaving off slices of turf from rival agencies and at defending its own turf against similar encroachments.

The CIA's concerns will probably be even more acute in cases where the target is a spy or terrorist who potentially could be dealt with through either law enforcement or intelligence tools.²⁹¹ Here, the cops' preferred method of prosecuting the suspect competes directly against the spies' approach of trying to flip him. For the CIA to assist an FBI criminal investigation in these circumstances would not just increase the Bureau's absolute amount of influence and autonomy. It would increase the Bureau's relative influence and autonomy at the expense of the CIA. In effect, CIA service as an FBI surrogate would have distributive consequences; it would precipitate a wealth transfer from the Agency to the Bureau. The CIA therefore will have intensified reasons not to collect criminal evidence on the FBI's behalf in the very national security cases in which the risk of pretextual surveillance is at its apogee.

CIA officials will have strong incentives not to do the FBI's bidding for a more practical reason, too: conducting surveillance for the Bureau almost certainly would violate the statutory injunction against exercising any "police, subpoena, or law enforcement powers" or performing any "internal security functions."²⁹² The outer limits of what the National Security Act of

289. Banks, *supra* note 37, at 1151.

290. See Sales, *supra* note 13, at 282–83 (explaining that intelligence officials seek to maximize their influence and autonomy, and that such conduct can contribute to interagency rivalries).

291. See Richard B. Schmitt & Greg Miller, *FBI Reportedly Widens Intelligence Gathering*, SEATTLE TIMES, Jan. 28, 2005, available at 2005 WL 1239108 (quoting a former senior CIA official expressing concern that FBI activity in traditional CIA domains such as counterterrorism constitutes a "battle for survival" for the Agency).

292. 50 U.S.C. § 403-4a(d)(1) (2006).

1947 proscribes may be ambiguous,²⁹³ but running wiretaps for the express purpose of uncovering evidence to be used in criminal proceedings satisfies anybody's definition of "law enforcement."²⁹⁴ To be sure, the Act does not make CIA law enforcement activity a criminal offense.²⁹⁵ But a statutory violation could still be costly; it could demoralize agency employees, alienate the President and other senior officials, and encourage rival agencies to poach CIA turf.²⁹⁶ Pretextual surveillance thus involves a striking asymmetry. The benefits of such surveillance would be externalized onto the FBI, but the costs would be internalized in the CIA. The cops have everything to gain; the spies have everything to lose. In light of that asymmetry, the CIA will have good reasons to refuse requests from FBI criminal investigators to conduct pretextual surveillance on their behalf.²⁹⁷

In fact, the risk of pretext under the 1947 Act is probably much lower than the risk of pretext under FISA. The USA PATRIOT Act may have increased the opportunities for FBI intelligence officials to engage in pretextual surveillance on behalf of FBI criminal investigators,²⁹⁸ but it is less likely that CIA intelligence officials and FBI criminal investigators will so collaborate. This is so because the internal rivalry between the Bureau's cops and spies appears to be less intense than the competition that characterizes FBI-CIA relations. The FBI's intelligence officials traditionally have come from the same law enforcement background as the Bureau's criminal investigators;²⁹⁹ FBI spies therefore may be more sympathetic to FBI cops' desire to collect evidence for criminal purposes than CIA spies would be. The weaker that rivalry, the more likely it is that the Bureau's spies would be willing to run wiretaps at the behest of the Bureau's cops. In short, there may be reasons to worry that PATRIOT's dismantling of the FISA wall could lead to improper coordination between the FBI's criminal and intelligence worlds. But those reservations don't justify information sharing limits between the FBI and CIA. Even if one rejects expanded coordination under FISA, it is still possible to embrace FBI-CIA data exchange to the extent it raises weaker pretext concerns.

Firewall Concerns

293. See *supra* notes 126–37 and accompanying text.

294. See, e.g., *Berger v. New York*, 388 U.S. 41, 60 (1967) (considering government assertion that wiretaps represent "a most important technique" for law enforcement).

295. See 50 U.S.C. § 403-4a(d)(1) (forbidding the CIA from engaging in "law enforcement," but not making it a crime to do so).

296. See *supra* note 75 and accompanying text.

297. In some circumstances, the CIA may calculate that the expected benefits of violating the 1947 Act exceed the expected costs. See *infra* text accompanying notes 304–24. But the CIA's benefits are unlikely to outweigh its costs when the unlawful surveillance is undertaken at the FBI's behest. See *supra* note 296 and accompanying text.

298. See *supra* text accompanying notes 105–19.

299. See POSNER, *supra* note 24, at 98–99 (discussing the mechanisms by which criminal investigators and intelligence officers are evaluated and how these performance criteria attract different personalities and talents).

The National Security Act of 1947 and the Posse Comitatus Act both reflect firewall values. Each seeks to isolate various aggressive national security operations that may be justified in some contexts and prevent them from contaminating other spheres where they are (at best) unjustified and (at worst) profoundly dangerous. The 1947 Act establishes a geographic and functional firewall; the CIA may operate overseas but not at home, and it may engage in intelligence but not law enforcement.³⁰⁰ Posse Comitatus, by contrast, distinguishes solely on the basis of functions; the Army and Air Force may engage in military operations but may not enforce civil laws.³⁰¹ Though the laws draw different lines, their basic rationale is the same—to prevent the CIA and the Armed Forces from undertaking violent operations in realms where they are inappropriate.

Information sharing seems to pose little risk of producing the grave firewall harms the 1947 Act and Posse Comitatus seek to avert. Data exchange is pretty far removed from the dangers those two statutes have in mind. What we worry about is the possibility that the CIA might eavesdrop on domestic political dissidents, manipulate elections, assassinate supposedly subversive political and civic leaders, and the like, not that the Agency might swap information with Homeland Security about al Qaeda operatives flying from Amsterdam to Detroit.³⁰² Similarly, we worry about heavily armed soldiers patrolling city streets like cops on the beat and deploying overwhelming violent force against fellow citizens as though they were enemies on the battlefield, not that the military might collaborate with the FBI in trying to pinpoint the location of an al Qaeda training camp in Yemen.³⁰³ It seems possible to have fairly robust information sharing between the CIA and domestic authorities on the one hand, and between the Armed Forces and civilian authorities on the other, without raising the firewall concerns embodied in the National Security Act and the Posse Comitatus Act.

In fact, a regime of expanded information sharing has the potential to vindicate firewall values more effectively than firm rules against coordinating with the CIA and the Armed Forces. This is so because data exchange can mitigate the incentives those agencies may experience to conduct surveillance or otherwise operate in ways that violate the 1947 Act or Posse Comitatus.

Imagine an intelligence system in which information sharing does not take place. Under such a regime, intelligence agencies will only gain access to the data they collect on their own. With sharing off the table, the CIA may face irresistible pressures to undertake domestic operations to gather information it has no other way to obtain. Suppose CIA analysts know that a

300. *See supra* notes 118–21 and accompanying text.

301. *See supra* notes 154–68 and accompanying text.

302. *See supra* notes 118–21 and accompanying text.

303. *See supra* notes 154–68 and accompanying text.

group of al Qaeda operatives has entered the country; the Agency wants to listen to their phone calls and read their e-mails in the hopes of discovering whether they are about to carry out an attack. The CIA can't ask the FBI to send over the communications the Bureau has intercepted, so the Agency has no alternative but to intercept the suspects' communications on its own. The same is true of the Armed Forces (although, as we will see in a moment, perhaps to a lesser extent). Suppose the Pentagon wants to learn the location of the training camp at which the al Qaeda members received instruction so it can strike the facility. Military brass can't ask the FBI for copies of the cell's intercepted communications, so they may want to gather the needed intelligence on their own—perhaps by running their own wiretaps, perhaps by sending undercover agents to observe the cell members at the mosque where they pray or the cafés they frequent.

In both cases, agencies' inability to rely on others for the intelligence they seek will incentivize them to mount operations that strike at the heart of the firewall values embodied in the National Security Act and the Posse Comitatus Act. CIA and military officials will engage in statutorily impermissible operations when they expect that the benefits of doing so will exceed the costs.³⁰⁴ The benefits side of the ledger is fairly straightforward. Among other factors, officials will weigh the tendency of the prohibited conduct to further the Agency's mission—in the CIA's case, tracking the al Qaeda cell and discerning its intentions; in the case of the military, locating and destroying the training camp. As for costs, officials will consider the opportunity cost of the unlawful surveillance—i.e., the value of the next-best choice that's given up in favor of independent surveillance. (In this hypothetical there is no next-best choice; the absence of information sharing means there is no other way for the agencies to obtain the intelligence they seek.) Officials also will weigh the expected harms of a statutory violation—public embarrassment, loss of agency influence, loss of agency turf, individual criminal liability, and so on—discounted by the probability that those violations will be detected. Those costs can be significant. The CIA and the military will not flout the 1947 Act and Posse Comitatus anytime they perceive a slight advantage—or even a significant advantage—of doing so. In many circumstances the expected costs of conducting statutorily impermissible operations will trump their expected benefits. But not always. The number of cases in which intelligence agencies calculate that unlawful operations are welfare enhancing can't be known with any precision, but it's probably greater than zero.

304. See WILSON, *supra* note 277, at xviii (explaining that some economists and political scientists apply utility maximizing theory to explain bureaucratic behavior).

For reasons of institutional self-interest and corporate culture,³⁰⁵ the military probably has weaker incentives to engage in prohibited law enforcement activities than the CIA has to engage in prohibited internal security operations. The Armed Forces traditionally have resisted Congress's calls to play a greater role in assisting law enforcement, such as in the fight against narcotics trafficking.³⁰⁶ Military brass fear, with some justification, that the institutional cop culture of scrupulous legalism will dull soldiers' battlefield instincts, resulting in less effective combat forces.³⁰⁷ Another reason for military officials' relatively weaker incentives to collect data in violation of the law is the prospect of individual criminal liability. A CIA official who violates the 1947 Act may get his agency in hot water, and his career prospects may suffer as a result, but he doesn't face any direct criminal sanctions.³⁰⁸ A military commander who directs his subordinates to engage in law enforcement functions, by contrast, may later be charged with violating the Posse Comitatus Act, a transgression that could land him in jail for up to two years.³⁰⁹

Information sharing can mitigate agencies' incentives to undertake prohibited operations. In effect, it functions as an escape valve, dissipating the pressures national security players may face to operate in statutorily prohibited spheres. If it is possible for the CIA and the Armed Forces to obtain the information they seek from, say, the FBI, there's less need for them to try to collect the data on their own—and therefore less risk that they will run afoul of firewall principles. Data exchange thus produces a substitution effect. Because information sharing is now an option, it's more costly for Langley and the Pentagon to gather data on their own in ways that could violate the 1947 Act or Posse Comitatus. In particular, information sharing increases the opportunity cost of engaging in independent surveillance in that it supplies a next-best alternative (and often a superior alternative). By increasing agencies' costs of conducting independent surveillance, data exchange reduces (even if it does not completely eliminate) their incentives to do so. Allowing the CIA and the Armed Forces to swap data with other intelligence agencies thus has the potential to vindicate firewall values even more effectively than a categorical prohibition on interagency coordination.

305. Cf. ZEGART, *supra* note 277, at 46–56 (using principles of organizational theory to explain behavior of intelligence agencies); Gregory S. McNeal, *Organizational Culture, Professional Ethics and Guantanamo*, 42 CASE W. RES. J. INT'L L. 125, 146 (2009) (same as to Armed Forces).

306. See Felicetti & Luce, *supra* note 151, at 150 (discussing Congress's attempt, as part of the 1982 DOD Authorization Act, to increase military and civilian law enforcement cooperation in the face of a worsening national drug problem, and the Pentagon's corresponding resistance).

307. See *supra* notes 167–74 and accompanying text.

308. See 50 U.S.C. § 403-4a(d)(1) (2006) (prohibiting CIA officials from exercising “police, subpoena, or law enforcement powers” but not providing any criminal penalties for violations).

309. See 18 U.S.C. § 1385 (2006) (providing that any person who “willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both”).

Republicanism Concerns

The Posse Comitatus Act seeks to preserve republicanism values—in particular, the notion that the Armed Forces must always be firmly subordinated to civilian authorities—in two distinct ways. First, by barring soldiers from participating in law enforcement, the Act prevents the military from exercising undue influence in civilian affairs.³¹⁰ Second, Posse Comitatus helps keep the military from developing an institutional perspective on law enforcement questions, thereby preserving independent domestic policy deliberations.³¹¹ These concerns are an insufficient basis for sharing restrictions. The expected costs of information sharing involving the Armed Forces are simply too small.

First, consider the costs of civilian authorities losing control of the Armed Forces. Expected cost is equal to the magnitude of the harm in question discounted by the probability that it will materialize.³¹² Such harms would be grave indeed; they would effectively mean an end to the American experiment in representative self-government. The flaw in this argument is that it is virtually impossible to imagine the military gaining undue influence in civilian affairs, let alone forcibly taking the reins of political power. The probability of such events coming to pass is miniscule, if not zero. And the likelihood that information sharing in particular will result in these harms is tinier still.

Whether military involvement in law enforcement aggrandizes the Armed Forces at the expense of civilian authorities is ultimately an empirical matter. There is not much data available on that question. But several anecdotes from centuries past to the modern era suggest that even direct military participation in basic law enforcement functions is unlikely to result in civilian authorities losing control of the Armed Forces. An early example is the Whiskey Rebellion. In 1794, the federal government raised and fielded an army to enforce a new tax on whiskey that rebellious farmers in western Pennsylvania refused to pay.³¹³ This was no ramshackle operation; the federal force was roughly the size of the Continental Army at its peak during the Revolutionary War, and President George Washington personally commanded it in the field.³¹⁴ Yet when the crisis passed, the militias were deactivated without incident and civilian authorities suffered no enduring

310. See *supra* notes 155–68, 179 and accompanying text.

311. See *supra* notes 175–91 and accompanying text.

312. See *United States v. Carroll Towing Co.*, 159 F.2d 169, 173 (2d Cir. 1947) (applying this principle to the question of negligence in tort liability).

313. Nigel Anthony Sellars, *Treasonous Tenant Farmers and Seditious Sharecroppers: The 1917 Green Corn Rebellion Trials*, 27 OKLA. CITY U. L. REV. 1097, 1104 (2002). See generally THOMAS P. SLAUGHTER, *THE WHISKEY REBELLION* (1986).

314. Sellars, *supra* note 314, at 1104–05.

loss of power.³¹⁵ Another example comes from the antebellum era. The Fugitive Slave Act of 1850 required officials to return to the South any slaves who escaped from bondage.³¹⁶ Sometimes the Army conducted the returns required by the Act.³¹⁷ Yet the Armed Forces did not thereby gain lasting independence from civilian leaders. More recently, and happily, President Eisenhower in 1957 deployed the Army's 101st Airborne Division to Little Rock, Arkansas, to ensure that African-American students were able to attend the city's public schools;³¹⁸ the Army was implementing the requirements of the Supreme Court's school-desegregation rulings.³¹⁹ Again, the Armed Forces' role in enforcing civil law didn't have any prolonged effect on the distribution of power between civilian and military officials. In short, the Armed Forces have been directed to engage in law enforcement activities repeatedly (if irregularly) over the course of American history, yet civilian authorities have not thereby ceded power to the Armed Forces. If these incidents are any indication, the slope to a military coup isn't that slippery after all.

It is even less likely that information sharing between military and law enforcement officials will result in the Armed Forces gaining independence and autonomy from civilian leadership. If the army's participation in collecting federal taxes, enforcing the terms of federal statutes, and implementing Supreme Court decisions didn't result in aggrandizement at the expense of the civilian sphere, it's hard to see how the considerably more benign swapping of data between the army and the FBI could. As argued above, information sharing can actually decrease the likelihood that the Armed Forces will engage in the sorts of core law enforcement activities that raise republicanism concerns.³²⁰ If the military is able to acquire the information it seeks from the FBI, it will have weaker incentives to collect on its own via independent law enforcement operations.³²¹ In short, the probability that data exchange will cause civilian authorities to lose control of the Armed Forces is fairly low, and the probability of a military coup is lower still.

What of the other threat to republicanism values the Posse Comitatus Act seeks to avert? There is some risk that participating in law enforcement

315. See ROBERT W. COAKLEY, *THE ROLE OF FEDERAL MILITARY FORCES IN DOMESTIC DISORDERS, 1789–1878*, at 64–68 (1988) (discussing Washington's use of militias to maintain order during the Whiskey Rebellion).

316. See Tkacz, *supra* note 173, at 321 (citing Act of Sept. 18, 1850, ch. 60, § 5, 9 Stat. 462, 462–63 (repealed 1864)).

317. *Id.* at 321–22.

318. KAREN ANDERSON, *LITTLE ROCK: RACE AND RESISTANCE AT CENTRAL HIGH SCHOOL 4* (2009).

319. See, e.g., *Brown v. Bd. of Educ. (Brown II)*, 349 U.S. 294, 301 (1955) (directing schools to desegregate “with all deliberate speed”).

320. See *supra* subpart II(B).

321. See *supra* notes 316–20 and accompanying text.

will cause the military to develop an institutional perspective on domestic policy questions, and that—owing to the high esteem in which the public holds the Armed Forces—voters and elected officials will extend undue deference to the military’s perspective in their policy deliberations.³²² The expected cost of this outcome is fairly low, too; the magnitude of the harm is simply too small to justify restrictions on information sharing.

This concern has to do with the quality of deliberations by voters and officeholders. The fear is not that the military will gain power at expense of civilians, but rather that civilian debate will suffer. From the standpoint of classical republicanism—an ideology that was in vogue at the time of the Founding³²³—the ideal political decision-making process involves citizens reaching conclusions based on an independent, disinterested, and rational weighing of competing conceptions of the public good.³²⁴ A corollary is that citizens must set aside extraneous considerations, such as their personal self-interest, the views of other parties, and so on. If too much weight is given to military opinion, the argument goes, that will distort the rational and independent deliberations called for by republicanism principles.³²⁵ Policy will be determined, not so much by an independent assessment that a certain course of action will advance the public good, but in part because voters are simply willing to take the military’s word for it.³²⁶ In effect, citizens might delegate some of their responsibility for making informed policy judgments to the Armed Forces.³²⁷

A lot can be said against this conception of political decision making, including wondering (as liberal theorists do) whether it is possible to conceive of a public good that is anything more than the sum of individual interests³²⁸ and questioning (as scholars of political ignorance do) whether

322. See, e.g., Richard H. Kohn, *The Erosion of Civilian Control of the Military in the United States Today*, 55 NAVAL WAR C. REV. 8, 9 (2002) (arguing that the Armed Forces have significant influence on the U.S. government’s policies).

323. See, e.g., Nathan Alexander Sales, *Classical Republicanism and the Fifth Amendment’s “Public Use” Requirement*, 49 DUKE L.J. 339, 349–50 (1999) (“During the final decades of the eighteenth century, republican theory . . . dominated the American political landscape.”).

324. See MICHAEL J. SANDEL, *DEMOCRACY’S DISCONTENT: AMERICA IN SEARCH OF A PUBLIC PHILOSOPHY* 5–6 (1996) (“According to republican political theory, however, sharing in self-rule . . . means deliberating with fellow citizens about the common good and helping to shape the destiny of the political community.”); GORDON S. WOOD, *THE CREATION OF THE AMERICAN REPUBLIC: 1776–1787*, at 55 (1969) (“By definition [republican government] had no other end than the welfare of the people: *res publica*, the public affairs, or the public good.”).

325. See Kohn, *supra* note 323, at 9 (“[T]he American military has grown in influence to the point of being able to impose its own perspective on many policies and decisions.”).

326. See *id.* at 17–19 (giving examples of how “senior military leaders have been able to use their personal leverage for a variety of purposes, sometimes because of civilian indifference, or deference, or ignorance”).

327. See *id.* at 19 (describing the interaction between the Armed Forces and the public as “a policy and decision-making process that has tilted . . . toward the military”).

328. See, e.g., Morton J. Horowitz, *Republicanism and Liberalism in American Constitutional Thought*, 29 WM. & MARY L. REV. 57, 68–69 (1987) (“The republican tradition promotes the

citizens actually engage in the deliberations assumed by republican principles.³²⁹ For our purposes, it is enough to say this: it doesn't seem any more problematic for citizens to defer to the opinions of military officials than it is for them to defer to the countless other institutions whose views they might consider when forming their own opinions.

Citizens don't deliberate in a vacuum. They are situated amid numerous organs of civil society—churches, charities, fraternal associations, and the like—and they commonly look to those institutions when forming their views on the hot-button issues of the day. Imagine a voter consulting the Catholic Church's teachings on the permissibility of capital punishment when deciding whether or not to support a legislative initiative to abolish the death penalty. The quality of public deliberations doesn't suffer from this kind of consultation. To the contrary, the existence of these institutional points of view may even enrich public debate, by exposing citizens to arguments they otherwise might not have considered. Moreover, a citizen's antecedent decision that she will defer to one organization and not to another is itself presumably the product of rational and independent deliberation that is fully consistent with republican values. When choosing whether to defer to Catholic, or Baptist, or Episcopalian teachings on capital punishment, our hypothetical voter by definition does not defer to those churches; deference comes into play only *after* the voter has decided—on her own—that a particular institution is worth listening to. And even if deference to civic institutions is thought to be undesirable in general, there is no reason to single out deference to the military as especially unwelcome. Republicanism may or may not be offended by citizens deferring to the views of their churches, of the charities to which they contribute, or of the fraternal associations to which they belong. But deference to the Armed Forces distorts the deliberative process neither more nor less than deference to these other institutions. (Again, recall that the concern here is not that the Armed Forces might acquire too much power, but rather that citizens will fail to engage in disinterested and independent deliberations.) In sum, the harms that data exchange could cause to republican values are both too remote and too small to justify sharing restrictions that segregate the military from law enforcement.

Privacy Concerns

Information sharing implicates the privacy concerns that lie at the heart of the Privacy Act—and also FISA and the National Security Act—in two distinct senses. First, sharing can undermine one's privacy interest in

concept of an autonomous public interest, whereas the liberal ideal holds that the public interest is either simply procedural or the sum of private interests.”).

329. See, e.g., Ilya Somin, *Political Ignorance and the Counter-majoritarian Difficulty: A New Perspective on the “Central Obsession” of Constitutional Theory*, 89 IOWA L. REV. 1287, 1303–05 (2004) (outlining the requirements of voter knowledge in deliberative democracy and claiming that American citizens are largely politically ignorant).

avoiding government observation of personal facts; it expands the circle of officials who are privy to one's private information.³³⁰ Second, sharing can undermine one's privacy interest in autonomously controlling the manner in which personal facts are presented to the outside world; it allows the government to use private information in ways that are far removed from the purposes for which the data originally was acquired.³³¹ Ultimately, privacy and information sharing are capable of peaceful coexistence; it is possible to achieve each without doing undue violence to the other. Information sharing generally poses less of a threat to personal privacy than surveillance does, and data exchange may preserve privacy values more effectively than sharing restrictions, by reducing agencies' incentives to engage in privacy-eroding surveillance.

I argued above that information sharing can undermine privacy interests.³³² That's true, but it is important to consider the relative magnitude of those privacy costs. Sharing is generally less harmful to privacy than surveillance is. The process of acquiring a given fact about a person via wiretap or physical search typically represents a greater affront to privacy than does the sharing of that same fact with other government officials after it has been acquired. This is so because surveillance inevitably involves the collection of extraneous and innocuous—and highly sensitive—data.³³³ When the FBI wiretaps a suspect's phone, it will not just overhear the suspect's incriminating conversations about bombmaking equipment, possible targets, sources of funding and training, and the identities of other co-conspirators. Agents also may overhear entirely innocent conversations that have no relevance to the investigation whatsoever—a conversation between the suspect and his mother in Yemen, a conversation between the suspect and a co-worker about the relative merits of the Redskins and the Cowboys, a conversation between the suspect's wife and their son's teacher about his progress in school, and so on. The process of locating individual grains of wheat that will be useful requires investigators to sift through massive amounts of chaff—sensitive and irrelevant personal facts concerning not just the suspect but other people with whom he comes into contact.³³⁴ By exposing investigators to these innocent and extraneous personal facts,

330. See *supra* notes 65–67 and accompanying text.

331. See *supra* notes 68–71 and accompanying text.

332. See *supra* notes 68–71 and accompanying text.

333. Nathan Alexander Sales, *Run for the Border: Laptop Searches and the Fourth Amendment*, 43 U. RICH. L. REV. 1091, 1130–31 (2009).

334. See, e.g., Rachel S. Martin, *Watch What You Type: As the FBI Records Your Keystrokes, the Fourth Amendment Develops Carpal Tunnel Syndrome*, 40 AM. CRIM. L. REV. 1271, 1289–90 (YEAR) (arguing that granting officials access to too much information can undermine personal privacy and interfere with communications protected by attorney–client privilege). But see Kent Walker, *Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange*, 2000 STAN. TECH. L. REV. 2, 26, <http://stlr.stanford.edu/pdf/walker-information-exchange.pdf> (“[I]n many cases, there’s an awful lot of wheat amidst the chaff.”).

surveillance can place severe strain on privacy values. (This is why FISA and Title III both require investigators to adopt “minimization” procedures—i.e., procedures designed to reduce the amount of innocent content that is collected and to destroy what innocent content is gathered.³³⁵)

The sharing of information among intelligence agencies usually will not produce privacy harms of this magnitude. A smaller amount of sensitive data changes hands under the typical information sharing arrangement than is acquired during typical surveillance. In many cases, intelligence agencies do not share their raw surveillance take with one another—the innocent conversations along with the incriminating.³³⁶ What are shared are the extracts—pieces of information that an analyst has processed, reviewed, and determined may be relevant to the investigation.³³⁷ As a result, an official with whom data is shared may learn nothing about the suspect’s mother, the co-worker’s football loyalties, or the teacher’s student evaluations; those conversations have been filtered out before the data reaches him. All the recipient encounters are the portions of the overheard conversations that indicate a terrorist plot may be afoot. The personal facts that intelligence agencies share often have been distilled down to their essence. They will not be accompanied by extraneous yet sensitive facts about the suspect and his circle of associates, which ordinarily will be left on the cutting room floor. So, yes, it’s true that information sharing can undermine personal privacy. But those harms need to be understood in context. Often the privacy costs of information sharing will be smaller—perhaps much smaller—than the privacy costs of outright surveillance.

In fact, an intelligence system based on widespread information sharing has the potential to vindicate privacy values even more effectively than a categorical ban on sharing. This is so because sharing can be a substitute for surveillance. In some circumstances—namely when officials deem the costs of wiretaps or physical searches to be excessive—intelligence agencies will prefer to acquire the information they seek from an interagency partner rather than by initiating a new round of surveillance. The sharing of previously gathered information thus can obviate the need for further privacy-eroding collection.

In an intelligence system whose members are free to swap data with each other, an agency that wishes to eavesdrop on a particular suspect’s communications will have, roughly speaking, two ways of doing so. It can either surveil the target on its own, or it can ask an interagency partner that

335. See 50 U.S.C. § 1801(h) (2006) (describing minimization procedures for FISA surveillance); 18 U.S.C. § 2518(5) (2006) (describing minimization procedures for criminal surveillance).

336. Intelligence agencies are reluctant to share their raw take for a number of reasons, including the need to protect the sensitive sources and methods they use to collect intelligence. See LOWENTHAL, *supra* note 24, at 75-76.

337. See *id.* at 55-67 (summarizing the intelligence-production cycle).

previously conducted surveillance of the target to hand over some of the resulting intercepts. Imagine that officials at Homeland Security are trying to decide whether to initiate electronic surveillance of two Brooklyn-based men. DHS wants to learn whether the men represent a threat to the Indian Point nuclear power plant, which is located just a few miles up the Hudson River from New York City. Officials know that, several weeks ago, the FBI ran wiretaps on the suspects' phones and also intercepted messages that were sent to and from their e-mail accounts. Will DHS engage in a fresh round of surveillance? Or will officials ask the Bureau to send them transcripts and recordings of the relevant phone calls, copies of the relevant e-mails, and the like?

In at least some cases, DHS will go with option two. Intelligence officials will choose to acquire the information they seek through data exchange when the net benefits of sharing (benefits minus costs) exceed the net benefits of fresh surveillance.³³⁸ Surveillance can be quite costly. If DHS initiates a new round of wiretaps, it will need to devote some of its finite resources to preparing an application to the FISA Court³³⁹ (and also to helping the Justice Department's Office of Intelligence Policy and Review shepherd the application through the FISA Court's approval process³⁴⁰). DHS officials will need to install and operate the taps, they may need to translate the overheard conversations and intercepted e-mails, and they will need to pore over the raw take, analyzing it for any signs of possible terrorist activity. A round of new surveillance also has opportunity costs. Every dollar and man-hour that DHS spends surveilling the Indian Point suspects is a dollar and man-hour that can't be spent investigating other possible threats. Sometimes the costs associated with fresh surveillance will be so great that DHS officials will prefer to obtain the information they want from their partners at the FBI.³⁴¹ In other words, the high cost of fresh surveillance will

338. See O'Connell, *supra* note 34, at 1675–90 (describing the costs and benefits associated with intelligence sharing).

339. See 50 U.S.C. § 1804 (2006) (outlining the application process and requirements for an order approving electronic surveillance).

340. See 9/11 COMMISSION REPORT, *supra* note 2, at 78 (noting that the Office of Intelligence Policy and Review is responsible for reviewing and presenting all FISA applications to the FISA Court).

341. For certain agencies, the costs of domestic surveillance in particular will be quite large, thereby systematically biasing them in favor of the information sharing alternative. For example, some agencies are legally prohibited from engaging in various forms of domestic surveillance, such as the CIA under the National Security Act of 1947 and the Army and Air Force under the Posse Comitatus Act. See *supra* subparts II(B) and II(C). For these agencies, the costs of surveillance will include another consideration—the expected cost of breaking the law (i.e., the magnitude of the harm associated with a statutory violation discounted by the probability it will be detected and punished). Because of these added costs, these agencies will tend to find information sharing even more attractive than fresh surveillance.

produce a substitution effect: agency officials will switch to the lower cost alternative of information sharing.³⁴²

It isn't possible to predict *a priori* how often intelligence agencies will decide to forego fresh surveillance in favor of information sharing. Nor is it easy to verify after the fact how often this substitution has taken place; much of the relevant data presumably remains shielded from public view by classification requirements. Still, it seems plausible that officials will prefer to obtain the information they seek via information sharing, rather than fresh surveillance, in a not-insignificant number of instances.³⁴³

The information sharing alternative imposes relatively weaker burdens on the suspects' privacy interests (and those of the people with whom they come into contact) than would be the case if a new batch of wiretaps were the only option. The targets will only be subject to one wiretap, not two. Investigators will not expose themselves to additional hours of sensitive and innocuous conversations in the hopes of discovering some new clue. If, on the other hand, data exchange is impossible—for instance, because the governing statute makes it unlawful—officials will have no real alternative but to collect the information by initiating yet another round of surveillance. This is not to say that there are *no* privacy costs associated with information sharing; plainly there are.³⁴⁴ The point I am making is a comparative one: that data exchange does a better job, relative to fresh surveillance, of preserving individual privacy.

Up to this point the analysis has focused entirely on a single kind of privacy interest—the data subject's interest in avoiding government observation. What about the other—the data subject's interest in controlling the manner in which his personal information is used? Information sharing can pit those two interests against each other. Sharing can promote a data subject's privacy interest in avoiding government observation because it reduces intelligence officials' incentives to subject him to additional rounds of privacy-eroding surveillance.³⁴⁵ But it does so precisely by violating that data subject's separate and distinct privacy interest in keeping his personal information from being widely disseminated without his knowledge or

342. Surveillance may be costly, but sharing can be costly too. Perhaps the most important cost of sharing is the opportunity cost of foregone surveillance. To stay with our hypothetical, if Homeland Security decides to forego new wiretaps and content itself with previously collected FBI data, there is a risk that an additional round of surveillance might have uncovered new information that isn't reflected in the existing FBI intercepts. In other words, the FBI may not have collected every last piece of data that's relevant to the DHS investigation; agency investigators might overhear something incriminating that the Bureau missed. Sometimes the opportunity cost of foregone surveillance will be so great as to prove decisive, tilting the balance in favor of fresh surveillance.

343. *Cf.* O'Connell, *supra* note 34, at 1675–76 (reporting that the 9/11 Commission advocated greater information sharing between intelligence agencies because it would, among other things, be less costly).

344. *See supra* notes 65–71 and accompanying text.

345. *See supra* notes 339–45 and accompanying text.

consent.³⁴⁶ When the Treasury Department provides the FBI with copies of a suspected terrorist's cancelled checks, it simultaneously protects the suspect from the Bureau independently rummaging through his bank records and causes the suspect to lose even more control over the uses to which his financial data are put. The vindication of the former interest depends on the violation of the latter. It's not privacy versus security, it's privacy versus privacy.

Candidly, this tradeoff—and the inevitable violation of privacy-as-control—seems an inescapable feature of information-sharing arrangements.³⁴⁷ By definition, sharing involves the dissemination of personal data to a wide range of players, almost always without the data subject's approval, and thus necessarily places strain on his privacy interest in controlling how his information is presented to others. But that is not a decisive objection to data exchange. Given the counterterrorism benefits of information sharing, we might be willing to tolerate some reduction in our ability to determine how our personal data is used. And the autonomy costs associated with information sharing might prove bearable since data exchange not only does not violate, but actually can preserve, the privacy interest in avoiding observation. In other words, the benefits of information sharing (improved counterterrorism and the protection of observational privacy) might outweigh the costs (violations of privacy-as-autonomy).

Even if the various privacy costs associated with information sharing are thought to be excessive, it might be possible to preserve privacy without resorting to outright restrictions on data exchange. Other potential safeguards may achieve an adequate level of privacy protection—or, to say something similar, a tolerable level of privacy infringement—while ensuring that the individual mosaic tiles circulate more or less freely among the nation's counterterrorism players.³⁴⁸ For instance, the Intelligence Community might make more extensive use of anonymization tools.³⁴⁹ Data that is to be shared with interagency partners (or even within a particular

346. See Bignami, *supra* note 69, at 669 (arguing that when government agencies collect, combine, and manipulate information on individuals without their consent, they “breach” the “essential liberal duty” of respecting citizens’ choices “to keep certain matters private and to make other matters public”); Dempsey & Flint, *supra* note 70, at 1462 (explaining that, in certain contexts, “privacy is about control, fairness, and consequences, rather than simply keeping information confidential”).

347. See Nehf, *supra* note 231, at 9–16 (describing the “modern database problem” as one in which people reveal their private data in order to reap the benefits and efficiencies of information sharing).

348. See generally Walker, *supra* note 334 (discussing the appropriate balance between privacy considerations and community benefits in information exchange).

349. See, e.g., Don Clark, *Entrepreneur Offers Solution For Security-Privacy Clash*, WALL ST. J., Mar. 11, 2004, at B1 (describing an innovative information-sharing system that makes information anonymous through “one-way hashing,” a mathematical technique that turns names, addresses, or other data into strings of digits that are almost impossible to convert back to their original form).

agency) could be scrubbed of all personally identifiable information, such as names and social security numbers, before it is sent to the recipient. The recipient would analyze the cleansed data, and would only need to learn individual identities if analysis turns up indications of possible terrorist activity.³⁵⁰ Or intelligence agencies could use immutable audit trails—i.e., computerized records that detail who has gained access to a particular piece of information.³⁵¹ Audit trails can be used to discipline agency personnel who have looked at personal information without adequate reasons—e.g., those who lack the necessary security clearances, or those whose job responsibilities don't provide the requisite "need to know."³⁵² Moreover, employees' awareness that audit trails exist, and that punishment awaits, might help deter them from improperly accessing personal data.

Conclusion

One lesson that virtually everyone took from 9/11 was the need to improve information sharing among the nation's national security players. Yet nearly a decade after those devastating terrorist attacks, a number of statutory walls continue to restrict the flow of data among intelligence, military, law enforcement, and other officials. The National Security Act of 1947, the Posse Comitatus Act, and the Privacy Act admirably seek to preserve fundamental policy values—the notions that cops shouldn't evade the legal limits on their surveillance powers by commissioning spies to do their dirty work for them, that spies and soldiers should restrict their violent tradecraft to spheres where it belongs, that civilian authorities must always be firmly in control of the Armed Forces, and that the government should strive to minimize harm to individual privacy. They do so, however, at a potentially significant cost to information sharing.

Fortunately, data exchange doesn't require us to discard the underlying principles on which these statutes are based. It's possible to preserve those values while at the same time increasing the flow of data among cops, spies, and soldiers. Indeed, information sharing can actually vindicate these principles more effectively than a categorical ban on data exchange. Pretext concerns generally don't necessitate limits on sharing between the FBI and CIA, since the latter's institutional self-interest naturally will predispose it

350. See MARKLE FOUND., *supra* note 244, at 146 (asserting that it would be prudent to "design systems that maintain practical anonymity for the subjects of [background] reviews"). *But see* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. (forthcoming 2010) (manuscript at 3), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006 (arguing that the privacy benefits of anonymization have been "vastly overstate[d]" because "[c]lever adversaries can often *reidentify* or *deanonymize* the people hidden in an anonymized database").

351. See, e.g., MARKLE FOUND., *supra* note 50, at 8 (recommending the use of immutable audit systems to facilitate both accountability and better coordination of analytical activities).

352. See MARKLE FOUND., *supra* note 244, at 16 ("Audit technology also facilitates tracking and monitoring to improve security and to prevent inappropriate access and use.").

against running wiretaps for the former's use in criminal proceedings. Data exchange among cops, spies, and soldiers may actually promote firewall values, by reducing incentives to use unsavory national security techniques in the domestic and law enforcement arenas. Republicanism concerns don't justify building an information-sharing wall around the Armed Forces, since the resulting harms are unlikely to occur. And information sharing can vindicate data subjects' privacy interests by mitigating incentives to engage in duplicative rounds of privacy-eroding surveillance.

Congress should follow its own example—the example it set in the USA PATRIOT Act—and dismantle these walls. As long as they remain on the statute books, the need for more information sharing may be a lesson we're condemned to learn over and over again.