



School of Law

MENDING WALLS: INFORMATION SHARING AFTER THE USA PATRIOT ACT

**Nathan Alexander Sales, Professor,
George Mason University School of Law**

Texas Law Review, Forthcoming

**George Mason University Law and Economics
Research Paper Series**

10-16

This paper can be downloaded without charge from the Social Science
Research Network at http://ssrn.com/abstract_id=1572984

MENDING WALLS:
INFORMATION SHARING AFTER THE USA PATRIOT ACT

Nathan Alexander Sales
George Mason University School of Law

ABSTRACT

The conventional wisdom is that the USA PATRIOT Act tore down the wall that prevented counterterrorism officials from sharing information with one another. Yet a number of laws remain on the books that could restrict data exchange, including the National Security Act of 1947, the Posse Comitatus Act, and the Privacy Act. Each statute reflects a blend of distinct policy concerns – for instance, preventing criminal investigators from evading the legal limits on domestic surveillance, keeping military and intelligence agencies from using excessive force in contexts where it’s unjustified, ensuring that the armed forces remain subordinate to civilian authorities, and safeguarding individual privacy against government intrusions. These laws are overbroad; they have the potential to restrict not just the harmful conduct Congress sought to proscribe, but also innocent information sharing. In fact, it’s possible to expand sharing while simultaneously vindicating these laws’ underlying principles. Intelligence agencies are unlikely to collect evidence for law enforcement officials to use in criminal proceedings, because doing so would undermine their institutional interests. Information sharing can mitigate intelligence and military incentives to operate in inappropriate spheres. The chances that data exchange might undermine civilian control of the military are too slight to justify sharing restrictions. And information sharing can preserve privacy values by reducing the need for agencies to engage in multiple rounds of privacy-eroding surveillance.

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”

TABLE OF CONTENTS

Introduction.....	1
I. Two Cheers for Information Sharing.....	4
II. Walls, Past and Present.....	10
A. The Life and Times of the FISA Wall.....	12
B. National Security Act of 1947.....	15
C. Posse Comitatus Act.....	19
D. Privacy Act.....	27
III. Recalibrating the Law and Policy of Information Sharing.....	31
A. Pretext Concerns.....	32
B. Firewall Concerns.....	35
C. Republicanism Concerns.....	37
D. Privacy Concerns.....	40
Conclusion.....	44

INTRODUCTION

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

[†] Assistant Professor of Law, George Mason University School of Law. Special thanks to the Center for Infrastructure Protection for generous financial support. I worked on a number of information-sharing initiatives while serving at the U.S. Departments of Justice and Homeland Security, but the opinions expressed in this article are solely mine.

¹ Fred F. Manget, *Intelligence and the Criminal Law System*, 17 STAN. L. & POL’Y REV. 415, 420 (2006) (“The wall is gone.”); RICHARD A. POSNER, PREVENTING SURPRISE ATTACKS: INTELLIGENCE REFORM IN THE WAKE OF 9/11 at 122 (2005) [hereinafter POSNER, SURPRISE ATTACKS] (arguing that the PATRIOT Act “accomplished” the goal of “eliminating artificial barriers to the pooling of intelligence data”).

It was the summer of 2001, and FBI agents were frantically trying to locate a suspected al Qaeda operative named Khaled al Mihdhar. Toward the end of August, Steve Bongardt, who was working the criminal investigation of U.S.S. *Cole* bombing, received an email 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 email: “Whatever has happened to this – someday somebody will die – and wall or not – the public will not understand why we are not more effective and throwing every resource we had at certain ‘problems.’”²

He was right. A few weeks later Khaled 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. The free flow of data, it was argued, would help them “connect the dots” and prevent future attacks. An early example of this consensus was the USA PATRIOT Act,³ which amended a provision in the Foreign Intelligence Surveillance Act that prevented intelligence officials at the FBI from exchanging data with criminal investigators.⁴ Yet even in PATRIOT’s wake, a number of walls remain on the statute books. 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.”⁵ 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 information 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

² NAT’L COMM’N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 270 (2004) [hereinafter 9/11 COMMISSION REPORT]; LAWRENCE WRIGHT, THE LOOMING TOWER: AL-QAEDA AND THE ROAD TO 9/11 at 353-54 (2007).

³ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

⁴ *Id.* § 218 (codified at 50 U.S.C. § 1804(a)(7)(B)).

⁵ Quoted in Grant T. Harris, *The CIA Mandate and the War on Terror*, 23 YALE L. & POL’Y REV. 529, 554 (2005).

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 exercising “police, subpoena, or law enforcement powers” or engaging in “internal security functions.”⁶ Similar to the FISA wall, the 1947 act 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 shouldn’t operate the same way domestically. The act could restrict the CIA’s ability to swap information with federal law enforcement officials, most notably at the FBI. A second restriction is found in the Posse Comitatus Act, 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”⁷ 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 – for example, by 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”⁸ – could prevent, for example, Customs from sharing data about arriving container ships with NSA officials who want to use 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’s possible to promote data exchange while remaining faithful to these laws’ underlying *pretext*, *firewall*, *republicanism*, and *privacy* concerns. The answer, I argue, is yes. The analysis is informed by rational-choice theories of bureaucratic action, and

⁶ 50 U.S.C. § 403-4a(d)(1).

⁷ 18 U.S.C. § 1385.

⁸ 5 U.S.C. § 552a(a)(7), (b)(3), (e)(4)(D).

focuses on individual and institutional incentives within military and intelligence agencies. It's unlikely that information sharing between the FBI and 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 interests. Similarly, sharing probably won't produce firewall harms. Data exchange can actually promote firewall principles by mitigating agencies' incentives to mount aggressive operations in inappropriate spheres. Republicanism concerns don't 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 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.⁹ 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.

I. 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.”¹⁰ Data exchange is worthwhile because it enables officials to piece together the intelligence mosaic, an especially important task in conflicts with nontraditional adversaries like terrorist organizations. Also, sharing produces efficiency gains by allowing different intelligence agencies to specialize in collecting particular kinds of information. 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.

⁹ See Nathan Alexander Sales, *Share and Share Alike: Intelligence Agencies and Information Sharing*, 78 GEO. WASH. L. REV. 279 (2010).

¹⁰ Noah Feldman, *Choices of Law, Choices of War*, 25 HARV. J.L. & PUB. POL'Y 457, 482 (2002); see also, e.g., Michael V. Hayden, *Balancing Security and Liberty: The Challenge of Sharing Foreign Signals Intelligence*, 19 NOTRE DAME J.L. ETHICS & PUB. POL'Y 247, 257-60 (2005); David S. Kris, *The Rise and Fall of the FISA Wall*, 17 STAN. L. & POL'Y REV. 487, 518, 521-22 (2006); Craig S. Lerner, *The USA PATRIOT Act: Promoting the Cooperation of Foreign Intelligence Gathering and Law Enforcement*, 11 GEO. MASON L. REV. 493, 524-26 (2003); POSNER, SURPRISE ATTACKS, *supra* note 1, at 26, 28; Richard Henry Seamon & William Dylan Gardner, *The PATRIOT Act and the Wall Between Foreign Intelligence and Law Enforcement*, 28 HARV. J.L. & PUB. POL'Y 319, 458-63 (2005); Peter P. Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 VILL. L. REV. 951, 951-59 (2006).

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. But seemingly innocuous data can become more meaningful, and more sinister, when aggregated with other information. This is known as the mosaic theory.¹¹ “[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.”¹² One tile may not suggest much at all, but the larger mosaic might. The mosaic theory traditionally has been offered as reason why the government might resist the release of a particular piece of information, as in response to a FOIA request.¹³ 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”¹⁴ – 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.”¹⁵

A related benefit is that information sharing can reduce the likelihood of catastrophic intelligence failures.¹⁶ “[T]he intelligence failures that hurt the worst have not been those of collection but rather those of dissemination.”¹⁷ Some scholars believe that breakdowns in information sharing contributed to our failure to anticipate the attack on Pearl Harbor. 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.¹⁸ Intelligence officers also determined that Japan had changed its naval call signs on November 1 and again on December 1,

¹¹ See generally David E. Pozen, Note, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628 (2005).

¹² *J. Roderick MacArthur Found. v. FBI*, 102 F.3d 600, 604 (D.C. Cir. 1996) (quoting *In re United States*, 872 F.2d 472, 475 (D.C. Cir. 1989)); see also *United States v. Marchetti*, 466 F.2d 1309, 1318 (4th Cir. 1972).

¹³ See, e.g., *CIA v. Sims*, 471 U.S. 159, 178 (1985) (upholding CIA’s refusal to divulge identities of private researchers participating in 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”).

¹⁴ NATHAN MILLER, *SPYING FOR AMERICA: THE HIDDEN HISTORY OF U.S. INTELLIGENCE* 5 (1989).

¹⁵ Letter from George Washington to Lord Stirling (Oct. 6, 1778), in 13 THE WRITINGS OF GEORGE WASHINGTON FROM THE ORIGINAL MANUSCRIPT SOURCES, 1745-1799, at 39, 39 (John C. Fitzpatrick ed., 1936); see also Hayden, *supra* note 10, at 258.

¹⁶ 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, *SURPRISE ATTACKS*, *supra* note 1, at 85-86; RICHARD A. POSNER, *UNCERTAIN SHIELD: THE U.S. INTELLIGENCE SYSTEM IN THE THROES OF REFORM* 22-29 (2006) [hereinafter POSNER, *UNCERTAIN SHIELD*]. 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 (4th ed. 2009). Enhanced information sharing may help stave off intelligence failure, but it doesn’t guarantee success.

¹⁷ Stewart A. Baker, *Should Spies Be Cops?*, FOREIGN POL’Y, Winter 1994-95, at 43.

¹⁸ ROBERTA WOHLSTETTER, *PEARL HARBOR: WARNING AND DECISION* 382, 385-86 (1962).

moves that were regarded “as signs of major preparations for some sort of Japanese offensive.”¹⁹ Yet these clues about Japan’s possible intentions were never pooled and integrated:

[N]o single person or agency had at any given moment all the signals existing in this vast information network. The signals lay scattered in a number of different agencies; some were decoded, some were not; some traveled through rapid channels of communication, some were blocked by technical or procedural delays; some never reached a center of decision.²⁰

Information sharing is also advantageous because it allows intelligence agencies to specialize in collecting different kinds of data, thereby producing efficiency gains.²¹ 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 the National Security Agency’s 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.²²) 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 – e.g., 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 won’t be disadvantaged by specializing; they will still, through a system of trade, have access to data collected by others. The result is to lower the intelligence system’s overall costs of producing assessments.

Sharing also has the potential to foster competitive analysis, which can result in better advice to policymakers. 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.²³ In other words, the nation’s three all-source agencies – CIA, the Defense Intelligence Agency, and the State Department’s Bureau of Intelligence and Research²⁴ – can incorporate into their intelligence assessments data that was gathered by, for instance, the FBI and the NSA. Information sharing can lead to the emergence of more all-source agencies. Sharing ensures that analysts aren’t limited to the data their own agency has managed to collect, but instead allows them to examine the widest possible range of

¹⁹ *Id.* at 385.

²⁰ *Id.* But see David Kahn, *The Intelligence Failure of Pearl Harbor*, FOREIGN AFFAIRS, Winter 1991-1992, at 138, 148 (“The intelligence failure at Pearl Harbor was not one of analysis, as Wohlstetter implies, but of collection.”).

²¹ Cf. POSNER, SURPRISE ATTACKS, *supra* note 1, at 14, 47.

²² See WRIGHT, *supra* note 2, at 382-88.

²³ See LOWENTHAL, *supra* note 16, at 72.

²⁴ See LOWENTHAL, *supra* note 16, at 38.

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. Previously I argued that redundant intelligence collection is inefficient, but not all redundancy is wasteful²⁵; 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 email. But redundant intelligence *analysis* can be beneficial. Competitive analysis helps ensure that policymakers are exposed to diverse perspectives; it also helps counteract groupthink tendencies.²⁶

Information sharing may produce even greater benefits in conflicts with terrorists than in traditional warfare between nation states.²⁷ 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 tanks to the border of West Germany. But asymmetric warfare often involves precursor acts that by themselves appear innocent.²⁸ 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. Their sinister implications can only be discerned when integrated with other pieces of information – e.g., intercepts suggesting that al Qaeda intended to use a Nigerian to attack the U.S. around the holidays, intercepted email traffic between Abdulmutallab and an anti-American cleric in Yemen, and warnings from Abdulmutallab's father that his son had become radicalized.²⁹ 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.

Widespread data exchange has the potential to harm the government's national security interests in several ways. Sharing increases the likelihood that a given piece of sensitive intelligence will be compromised, whether through espionage (acquisition by a foreign power) or leaks (disclosures to unauthorized persons, such as the news media). 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 agencies. But in both cases there is a compelling safety rationale."³⁰

²⁵ 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, 1675-54 (2006) (discussing some costs and benefits of redundancy among intelligence agencies).

²⁶ See William C. Banks, *And the Wall Came Tumbling Down: Secret Surveillance After the Terror*, 57 U. MIAMI L. REV. 1147, 1151, 1193 (2003) [hereinafter Banks, *Secret Surveillance*]; LOWENTHAL, *supra* note 16, at 14, 139; O'Connell, *supra* note 25, at 1676, 1689, 1731-32. Competitive analysis also has its downsides. "The existence of an alternative analysis, especially on controversial issues, can lead policymakers to shop for the intelligence they want or cherry-pick analysis, which also results in politicization." LOWENTHAL, *supra* note 16, at 135.

²⁷ See Swire, *supra* note 10, at 955-57.

²⁸ See LOWENTHAL, *supra* note 16, at 133.

²⁹ See Eric Lipton et al., *Review of Jet Bomb Plot Shows More Missed Clues*, N.Y. TIMES, Jan. 17, 2010, at __; Mark Hosenball et al., *The Radicalization of Umar Farouk Abdulmutallab*, NEWSWEEK, Jan. 11, 2010, at __.

³⁰ POSNER, SURPRISE ATTACKS, *supra* note 1, at 103.

Still, the risk that sharing might compromise sensitive data seems exaggerated. Cold War era information-access standards like compartmentalization rules and “need to know” requirements were designed to counter a particular type of threat: espionage by a traditional nation-state adversary like the Soviet Union. They may be less vital in today’s era of asymmetric conflicts with international terrorists. Sharing restrictions still play an important role in preventing espionage by rival nations, such as Iran or North Korea. But terrorist groups like al Qaeda have not proven as adept at placing spies in the American intelligence community.³¹ At least as to information related to terrorist threats, then, the risks of espionage seem weaker.³² 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, the secret CIA prisons in Central Europe, and so on.³³ But it might be possible to mitigate those risks with countermeasures other than sharing restrictions, such as electronic audit trails that record which officials have accessed a particular piece of information.³⁴

Sharing also can harm national security by producing a “flooding effect” – i.e., by inundating analysts with massive amounts of information. Roberta Wohlstetter argues that intelligence analysis is akin to trying to locate a faint “signal” hidden amid a mass of “noise.”³⁵ 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 weren’t swamped with data.³⁶ 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.³⁷ In other words, sharing can exacerbate confirmation bias. 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 don’t. The result is analytical ossification, as established theories are reinforced and alternatives go unnoticed.

³¹ *But see* Richard A. Oppel Jr., et al., *Attacker 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 double agent).

³² *Cf.* POSNER, UNCERTAIN SHIELD, *supra* note 16, at 215 (indicating that, while “[f]oreign states have their own intelligence agencies that can steal secrets by pooling and analyzing scattered bits of information obtained from leaks or moles,” terrorist organizations “have much less elaborate intelligence apparatus,” and arguing that classifying information “is not responsive” to the threat posed by terrorists).

³³ *See, e.g.*, James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1; Dana Priest, *CIA Holds Terror Suspects in Secret Prisons*, WASH. POST., Nov. 2, 2005, at A01.

³⁴ *See* MARKLE FOUND., MOBILIZING INFORMATION TO PREVENT TERRORISM: ACCELERATING DEVELOPMENT A TRUSTED INFORMATION SHARING ENVIRONMENT, THIRD REPORT OF THE MARKLE FOUNDATION TASK FORCE 1-3, 6-7 (2006) [hereinafter THIRD MARKLE REPORT].

³⁵ *See* WOHLSTETTER, *supra* note 18, at 387, 393.

³⁶ *Cf.* WOHLSTETTER, *supra* note 18, at 387 (“We failed to anticipate Pearl Harbor not for want of the relevant materials, but because of a plethora of irrelevant ones.”).

³⁷ *See* POSNER, SURPRISE ATTACKS, *supra* note 1, at 116-17.

Concerns about flooding are legitimate, but they don't justify wholesale limits on information sharing. It's true that analysts' cognitive limitations are an imperfect way to filter data. But so are sharing restrictions. In a system that uses sharing limits as a filter, what determines whether data from one agency reaches another is not an informed, disinterested judgment about whether or not it would be useful. 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.³⁸ 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. CIA reportedly is developing image-recognition technology that enables computers to match photographs with exemplars stored in a database.³⁹ 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.⁴⁰ And computers are often tasked with running keyword queries ("al Qaeda," "jihad," and the like) against intercepted phone calls and emails. Human beings would only need to inspect what passed the automated filters. (Still, this seems an imperfect solution to the flooding effect. "Even in the age of computers, few technical shortcuts have been found to help analysts deal with the problem."⁴¹)

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.⁴² Specifically, information sharing interferes with one's interest in preventing the government from observing personal facts.⁴³ The sharing of 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. 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.⁴⁴

³⁸ See generally Sales, *supra* note 9.

³⁹ See LOWENTHAL, *supra* note 16, at 73.

⁴⁰ See Walter Pincus, *Finding a Way to Review Surveillance Tape in Bulk*, WASH. POST., Mar. 10, 2009, at A11.

⁴¹ LOWENTHAL, *supra* note 16, at 117.

⁴² *Contra* Kris, *supra* note 10, at 520 (arguing that sharing restrictions "do[] not provide much protection for privacy").

⁴³ See, e.g., Julie E. Cohen, *Examined Lives, Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1371, __ (2000).

⁴⁴ Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PENN. L. REV. 477, 507 (2006); cf. Patricia L. Bellia, *The Memory Gap in Surveillance Law*, 75 U. CHI. L. REV. 137, 139 (2008).

This is the same insight that informs the mosaic theory: Integration creates new information. 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.

In addition to 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 control the dissemination of information about themselves 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.”⁴⁵

The problem here is not so much that information sharing prevents data subjects from keeping personal information confidential; the problem is that sharing has the potential to undermine data subjects’ autonomy.⁴⁶ 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.⁴⁷

II. WALLS, PAST AND PRESENT

The USA PATRIOT Act may have brought down one wall, but a number of others remain on the statute books. This section begins with a brief discussion of the FISA wall, then surveys the remaining statutory limits on information sharing as well as their underlying policy values. 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.⁴⁸

⁴⁵ 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, 458-58 (1995) (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) [hereinafter Bignami, *Transnational Intelligence*].

⁴⁶ See James X. Dempsey & Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459, 1462 (2004).

⁴⁷ See *infra* Part III.C.

⁴⁸ Several other statutes have the potential to restrict information sharing, but don’t 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 (prohibiting any “officer or employee of the United States” from “publish[ing], divulg[ing], disclos[ing], or mak[ing] known in

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 these laws. Sometimes they were – the Privacy Act quite obviously was intended to preserve individual privacy – but sometimes they weren’t. 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. 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

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. *See* HSA § 214(e)(1), (2)(D) (directing Secretary of Homeland Security to “establish uniform procedures for the receipt, care, and storage by Federal agencies of critical infrastructure information,” including mechanisms “to permit the sharing of such information within the Federal Government”). 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 and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or for another informational purpose including, without limitation, the identification, analysis, prevention, preemption, and/or disruption of terrorist threats to our homeland.” 6 C.F.R. § 29.8(b). *See* *Chrysler Corp. v. Brown*, 441 U.S. 281, 306-11 (1979) (holding that validly promulgated regulations can amount to legal authorization within meaning of 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. However, the HIPAA privacy rule, promulgated by the Department of Health and Human Services in 2000, doesn’t 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. *See* Peter P. Swire & Lauren Steinfeld, *Security and Privacy After September 11: The Health Care Example*, 86 MINN. L. REV. 1515, (2002). 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) (exceptions for “public health activities,” “law enforcement purposes,” and where necessary to “avert a serious threat to health or safety”).

statutory charter can demoralize employees, decreasing their productivity. It can render the agency politically radioactive, resulting in the president and other senior policymakers keeping it at arm's length. And it can encourage bureaucratic rivals to poach a weakened agency's turf.⁴⁹ In short, it doesn't 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.

A. The Life and Times of the FISA Wall

The most notorious wall traces its roots to an obscure provision in the Foreign Intelligence Surveillance Act.⁵⁰ 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.⁵¹ Among various requirements, FISA directed the government to certify to the court that "the purpose" of the proposed surveillance was to gather foreign intelligence.⁵² 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. If, on the other hand, the government's objective was principally to enforce domestic criminal laws, it would have to satisfy the ordinary (and relatively strict) standards that govern garden variety criminal investigations. At some point in the 1980s, the Justice Department began to read FISA as requiring that "the primary purpose" of the proposed surveillance must be to collect foreign intelligence.⁵³ (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.⁵⁴)

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. The more information that changed hands 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

⁴⁹ 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. CIA lost some of its pull with the White House – witness the administration's decision, over CIA objections, to release Justice Department memoranda on the legality of coercive interrogation. See Mark Mazetti & Scott Shane, *Interrogation Memos Detail Harsh Tactics by the C.I.A.*, N.Y. TIMES, Apr. 17, 2009, at A1. And 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. See Anne E. Komblut, *Obama Approves New Team to Question Terror Suspects*, WASH. POST, Aug. 25, 2009, at ___.

⁵⁰ For detailed histories of the FISA wall see, e.g., 9/11 COMMISSION REPORT, *supra* note 2, at 78-80; Banks, *Secret Surveillance*, *supra* note 26, at 1153-88; Kris, *supra* note 10, at 499-518.

⁵¹ See 50 U.S.C. § 1804.

⁵² See *id.* § 1804(a)(7)(B).

⁵³ See *In re: Sealed Case*, 310 F.3d 717, ___ (2002).

⁵⁴ *United States v. Truong*, 629 F.2d 908, ___ (4th Cir. 1980).

collecting foreign intelligence. 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.⁵⁵ 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.” As such, DOJ 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.”⁵⁶ (The FISA wall thus was not just a statutory restriction; it derived from administrative interpretations and judicial decisions, as well as the underlying statute itself.) As a result, information sharing essentially ground to a halt.⁵⁷

Why was the FISA wall built in the first place? As the Justice Department’s 1995 guidelines indicate, the justification was the need to prevent officials from evading the legal limits on domestic surveillance. 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. Let’s call this a *pretext* concern. (By maintaining the legal limits on domestic surveillance, the FISA wall also sought to preserve the privacy interests of persons subject to surveillance. A good deal more will be said about privacy below.⁵⁸)

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.⁵⁹ 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.”⁶⁰ 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

⁵⁵ See, e.g., Memorandum from Janet Reno, Attorney General, to Assistant Attorney General et al. (July 19, 1995) § (A)(6), available at <http://www.fas.org/irp/agency/doj/fisa/1995procs.html>; Memorandum from Jamie S. Gorelick, Deputy Attorney Gen., to Mary Jo White, United States Attorney, S. Dist. N.Y., et al., Instructions on Separation of Certain Foreign Counterintelligence and Criminal Investigations (DATE?) 2, available at <http://www.cnss.org/1995%20Gorelick%20Memo.pdf> [hereinafter Gorelick Memo].

⁵⁶ Gorelick Memo, *supra* note 55, at 2, 3.

⁵⁷ The Justice Department directives established a mechanism by which information might be shared, see Gorelick Memo, *supra* note 55, at 3, but in practice very little data ended up changing hands, see 9/11 COMMISSION REPORT, *supra* note 2, at 78-79.

⁵⁸ See *infra* Parts II.D, III.D.

⁵⁹ Cf. *United States v. United States District Court*, 407 U.S. 297, ___ (1972) (citing “potential distinctions” between “criminal surveillances and those involving the domestic security”).

⁶⁰ Orin S Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn’t*, 97 Nw. U. L. Rev. 607, ___ (2003)

establish probable cause to believe a crime has been, is being, or is about to be committed.⁶¹ 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”⁶² – in layman’s terms, a spy or a terrorist. The standards are looser still for intelligence collection overseas. The Fourth Amendment may not apply at all to noncitizens who aren’t present in the United States – not just the warrant requirement, but the entire Fourth Amendment, including the requirement of reasonableness.⁶³ 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.

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 intercepts for use in criminal investigations. 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. 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. The FISA wall thus amounted to a prophylactic rule.⁶⁴ It proscribed not just the specific harm that DOJ sought to avert (cops evading the legal limits on domestic surveillance by issuing tasking orders to spies), but also related conduct that could either be wholly innocent or could be the first tentative steps toward an impermissible tasking.

⁶¹ See 18 U.S.C. § 2518(3)(a), (3)(c), (5).

⁶² See 50 U.S.C. §§ 1801(a) & (b), 1805(a)(3).

⁶³ See, e.g., *United States v. Verdugo-Urquidez*, 494 U.S. 259, 261-65 (1990). *But see* *Boumediene* (establishing “functional test” to determine whether aliens detained outside United States have constitutional right to seek writs of habeas corpus).

⁶⁴ 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”); see also David A. Strauss, *The Ubiquity of Prophylactic Rules*, 55 U. CHI. L. REV. 190, 190 (1988).

The wall eventually came down. Section 218 of the USA PATRIOT Act abolished the primary purpose test, substituting a new requirement that “a significant purpose” of proposed FISA surveillance must be to collect foreign intelligence.⁶⁵ As a result, FISA 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). FISA also would still be a viable option even if the spies and cops talked to one another about their respective approaches to the case. Section 504 was even blunter; it provided that intelligence officials “may consult with Federal law enforcement officers to coordinate efforts” against national security threats.⁶⁶ Many academics take a dim view of these changes, arguing that PATRIOT enables officials to engage in what I’m calling pretextual surveillance.⁶⁷ The FISA court shared some of those concerns, but in 2002 the FISA court of review upheld the amended FISA against a constitutional challenge.⁶⁸

B. 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, granting it certain powers and denying it certain others. As relevant here, the CIA is denied any “police, subpoena, or law enforcement powers or internal security functions.”⁶⁹ 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.

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. Intelligence is 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. 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,

⁶⁵ USA PATRIOT Act § 218 (codified at 50 U.S.C. § 1804(a)(7)(B)). 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 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)

⁶⁶ USA PATRIOT Act § 504 (codified at __).

⁶⁷ *See, e.g.*, Banks, *Secret Surveillance*, *supra* note 26, at 1150; Erwin Chemerinsky, *Losing Liberties: Applying a Foreign Intelligence Model to Domestic Law Enforcement*, 51 UCLA L. REV. 1619, 1624-27 (2004); 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, __ (2003); George P. Varghese, *A Sense of Purpose: The Role of Law Enforcement in Foreign Intelligence Surveillance*, 152 U. PA. L. REV. 385, 386 (2003).

⁶⁸ *See In re: Sealed Case*, 310 F.3d 717, __ (2002).

⁶⁹ 50 U.S.C. § 403-4a(d)(1).

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.⁷⁰ 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. The standard account is true enough, but incomplete in one important respect. It doesn’t appear that Congress wanted to ban the use of aggressive intelligence techniques per se. 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, or 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. 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,” 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.⁷¹ (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.⁷²) 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 mounting certain kinds of domestic operations – and perhaps even from sharing information concerning certain domestic operations – there are fewer opportunities for officials to evade the ordinary restrictive rules that govern criminal investigations. (The seal isn’t watertight; Executive Order 12333 authorizes the CIA to undertake a variety of domestic operations, such as protecting agency facilities and personnel against various threats.⁷³)

⁷⁰ See, e.g., Sherri J. Conrad, *executive Order 12,333: “Unleashing” the CIA Violates the Leash Law*, 70 CORNELL L. REV. 968, 975 (1985); Jonathan M. Fredman, *Intelligence Agencies, Law Enforcement, and the Prosecution Team*, 16 YALE L. & POL’Y REV. 331, 335 (1998); Harris, *supra* note 5, at 531; Frederick P. Hitz, *Unleashing the Rogue Elephant: September 11 and Letting the CIA Be the CIA*, 25 HARV. J.L. & PUB. POL’Y 756, 769 (2002); Manget, *supra* note 1, at __; Daniel L. Pines, *The Central Intelligence Agency’s “Family Jewels”: Legal Then? Legal Now?*, 84 IND. L.J. 637, 640 (2009).

⁷¹ See *supra* notes 58 to 64 and accompanying text.

⁷² See *infra* Parts II.D, III.D.

⁷³ See Exec. Order 12,333 § 1.8(h).

How does the 1947 act give concrete form to these firewall and pretext policy concerns? Badly. The terms of the statutory prohibition on “police, subpoena, or law enforcement powers or internal security functions”⁷⁴ are notoriously ambiguous. In 1976, the Church Committee called the provision “confusing and ill-defined.”⁷⁵ 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,”⁷⁶ and even the agency’s former general counsel confesses that “the limits on what the CIA can and cannot do are not clear.”⁷⁷ Nor has the judiciary offered much assistance; “[c]ourts have generally eschewed clear definitions and parameters on CIA domestic activity.”⁷⁸ Because of its indeterminacy, the 1947 act is amenable to any number of competing interpretations. A strict reading of “internal security,” championed by some,⁷⁹ would exclude the CIA from virtually any domestic responsibilities whatsoever. The flexible reading favored by others⁸⁰ would preserve at least some domestic responsibilities for the agency.

Who’s right? The answer matters a great deal. Depending on how it’s interpreted, the internal-security ban could impose severe restrictions on information sharing between the CIA and the FBI and other domestic entities.⁸¹ 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.⁸² 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 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.⁸³) The 1947 act might forbid the data exchange on which this sort of collaboration depends.

Consider the flow of information from the CIA to FBI. The FBI isn’t just responsible for domestic intelligence; it’s also the nation’s preeminent law-enforcement agency. That means the bureau may want to use a given piece of information for intelligence purposes, but it also may

⁷⁴ 50 U.S.C. § 403-4a(d)(1).

⁷⁵ 1 Church Committee Report at 436.

⁷⁶ Conrad, *supra* note 70, at 971.

⁷⁷ Harris, *supra* note 5, at 533 (quoting Jeffrey H. Smith, former CIA general counsel).

⁷⁸ Harris, *supra* note 5, at 534.

⁷⁹ See, e.g., Conrad, *supra* note 70, at 973 & n.35, 975, 976.

⁸⁰ See Harris, *supra* note 5, at 547.

⁸¹ See Conrad, *supra* note 70, at 988.

⁸² See Sales, *supra* note 9, at 303-13; *infra* notes 171 to 173 and accompanying text.

⁸³ See *supra* notes 21 to 22 and accompanying text.

want to use the same data in criminal proceedings; the information is “dual use.” Suppose the CIA hands the FBI intelligence information it collected overseas. If the bureau intends to use it in a criminal prosecution, CIA becomes an active participant in the collection of evidence for use at trial.⁸⁴ 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? 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[.]”

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:

[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.⁸⁵

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 helps apprehend terrorists and others wanted by the FBI. 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.⁸⁶ CIA taking bin Laden into custody might count as “law

⁸⁴ Depending on the arrangement, the FBI might be barred from using CIA-originated information in criminal proceedings without CIA’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 16, at 154.

⁸⁵ <http://www.justice.gov/ag/readingroom/guidelines.pdf>

⁸⁶ See WRIGHT, *supra* note 2, at ___.

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. The 1947 act similarly might rule out information sharing about such apprehensions. Suppose the FBI captures bin Laden itself after being tipped off by CIA analysts that he’s 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 mere possibility of criminal proceedings convert CIA’s information sharing into “law enforcement” in violation of the 1947 act?⁸⁷

Again, the point is not that 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”⁸⁸ isn’t a model of clarity, and it’s far from certain which types of data exchange are permitted and which are forbidden. But that isn’t 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.⁸⁹

C. 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.”⁹⁰ *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.”⁹¹ The Posse Comitatus Act is one of the more venerated laws in the U.S. Code. From an information-sharing standpoint, it’s also one of the more vexing; its strict but ambiguous limits could interfere with the exchange of data between law enforcement authorities and the armed forces.

⁸⁷ Section 905 of the USA PATRIOT Act might permit some of these information sharing initiatives, but it isn’t a slam dunk. That 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 § 905. But section 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. It therefore wouldn’t override any restriction in the 1947 act on CIA sending information to counterparts at law-enforcement agencies. Second, and more importantly, section 905 only permits sharing “[e]xcept as otherwise prohibited by law.” That reservation clause might maintain any information-sharing limits required by CIA’s statutory charter.

⁸⁸ 50 U.S.C. § 403-4a(d)(1).

⁸⁹ See *supra* note 49 and accompanying text.

⁹⁰ 18 U.S.C. § 1385.

⁹¹ DELUXE BLACK’S LAW DICTIONARY 1162 (6th ed. 1990).

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 in other settings. 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. 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.⁹² (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. In 1878 they managed to persuade the rest of Congress to enact their preferences into law.⁹³) 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 policy⁹⁴) – should be kept separate from the world of law enforcement. The act thus serves to insulate criminal investigations from the more violent practices and rules of engagement that characterize military operations. This firewall concern is similar to the rationale for Congress’s decision in the National Security Act of 1947 largely to exclude CIA from domestic operations. But there’s a subtle difference. The 1947 act draws both a *geographic* line of demarcation (CIA may operate overseas but not in the United States) and a *functional* one (CIA may engage in intelligence but not law enforcement). Posse Comitatus, by contrast, draws only a *functional* line. The armed forces may undertake military functions but they may not assume law enforcement responsibilities.

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. The military subdues enemy forces through overwhelming violence. 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.⁹⁵ Another important difference

⁹² 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).

⁹³ See, e.g., Candidus Dougherty, “Necessity Hath No Law”: *Executive Power and the Posse Comitatus Act*, 31 CAMP. L. REV. 1, 12-14 (2008); Gustav Eyster, *Gangs in the Military*, 118 YALE L.J. 696, 718 (2009); Felicetti & Luce, *supra* note 92, at 100-13.

⁹⁴ See Michael Greenberger, *Did the Founding Fathers Do “A Huckuva 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); Joshua M. Samek, *The Federal Response to Hurricane Katrina: A Case for Repeal of the Posse Comitatus Act or a Case for Learning the Law?*, 61 U. MIAMI L. REV. 441, 446 (2007).

⁹⁵ See 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) [hereinafter Banks, *Homeland Security*]; Nathan Canestaro, *Homeland Defense: Another Nail in the Coffin for Posse Comitatus*, 12 WASH. U. J.L. & PUB. POL’Y 99, 100, 140-41 (2003); Sean J. Kealy, *Reexamining the Posse Comitatus Act: Toward a Right to Civil Law Enforcement*, 21 YALE L. & POL’Y REV. 383, 386 (2003); Diane Cecilia Weber, *Warrior Cops: The*

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. 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.⁹⁶ Battlefield rules of engagement seek to maximize military effectiveness; the rules governing criminal investigations seek to constrain, to prevent officers from investigating, arresting, and detaining too aggressively.⁹⁷ The Posse Comitatus Act thus prevents military mores and 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 will be diverted away from their core mission of fighting wars.⁹⁸ There’s also a more immediate risk that law-enforcement responsibilities will blunt the military’s combat readiness. 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.”⁹⁹

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. The founding generation’s apprehensions about standing armies are well known and needn’t be rehearsed at length here.¹⁰⁰ 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!”¹⁰¹ 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

Ominous Growth of Paramilitarism in American Police Departments 1, 10 (1999), <http://www.cato.org/pubs/briefs/bp50.pdf>.

⁹⁶ See, e.g., *Tennessee v. Garner*, 471 U.S. 1 (1985).

⁹⁷ See Kealy, *supra* note 95, at 386-87; Weber, *supra* note 95, at 2-3.

⁹⁸ See Kealy, *supra* note 95, at 420-21.

⁹⁹ Banks, *Homeland Security*, *supra* note 95, at 771.

¹⁰⁰ See, e.g., Canestaro, *supra* note 95, at 105; Dougherty, *supra* note 93, at 4-8; Kealy, *supra* note 95, at 391.

¹⁰¹ John Adams, *Argument*, in 3 LEGAL PAPERS OF JOHN ADAMS 266 (1965).

any military intrusion into civilian affairs.”¹⁰² More specific still is the principle that the military should play no role in the enforcement of civil laws.¹⁰³

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. 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 – and 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 percent of adults reported having “a great deal” or “quite a lot” of confidence in the military. The military scored 15 points higher than the next most popular choice (small business, weighing in at 67 percent), and it trounced such also-rans as the presidency (51 percent), the Supreme Court (39 percent), and Congress (17 percent!).¹⁰⁴ It’s 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 they’re 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 place. 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 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

¹⁰² *Laird v. Tatum*, 408 U.S. 1, 15 (1972); see also Banks, *Homeland Security*, *supra* note 95, at 740; Scott R. Tkacz, *In Katrina’s Wake: Rethinking the Military’s Role in Domestic Emergencies*, 15 WM. & MARY BILL RTS. J. 301, at 307 (2006). But see Felicetti & Luce, *supra* note 92, at 93 (“While the nation’s founders were deeply concerned with the abuses of the British Army during 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.” (footnote omitted)).

¹⁰³ See Banks, *Homeland Security*, *supra* note 95, at 740; Canestaro, *supra* note 95, at 99 (act “uph[o]ld[s] 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).

¹⁰⁴ <http://www.pollingreport.com/institut.htm>.

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.” The act is plagued by ambiguity.¹⁰⁵ Some commentators say the act bars a fairly wide range of conduct,¹⁰⁶ while others think it doesn’t rule out much at all.¹⁰⁷ How to construe the act is of more than academic interest, because criminal penalties await those who violate it. No one has ever been prosecuted under the act,¹⁰⁸ but uncertainty about its scope and the mere threat of criminal sanctions can deter military officials from taking actions that may well be lawful.¹⁰⁹

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. Indeed, in part because of the act, military brass appear to be exceedingly reluctant to share information with their colleagues in law-enforcement agencies.¹¹⁰ A series of hypotheticals should help illustrate why.

Imagine that al Qaeda carries out a catastrophic terrorist attack – 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, 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”¹¹¹ within the meaning of the Posse Comitatus Act for the military to give imagery,¹¹² forensic analysis, and other types of information to a law

¹⁰⁵ See Linda Demaine & Brian Rosen, *Process Dangers of Military Involvement in Civil Law Enforcement: Rectifying the Posse Comitatus Act*, 9 N.Y.U. J. L. & PUB. POL’Y 167, 170 (2005); Felicetti & Luce, *supra* note 92, at 88; Tkacz, *supra* note 102, at 309.

¹⁰⁶ See, e.g., Canestaro, *supra* note 95.

¹⁰⁷ See, e.g., Dougherty, *supra* note 93, at 15; Felicetti & Luce, *supra* note 92, at 119-20; Greenberger, *supra* note 94, at 401.

¹⁰⁸ See Kealy, *supra* note 95, at 405.

¹⁰⁹ See *supra* note 49 and accompanying text.

¹¹⁰ See, e.g., Eyler, *supra* note 93, at 717-18; Kealy, *supra* note 95, at 432.

¹¹¹ 18 U.S.C. § 1385.

¹¹² Cf. *White House to Abandon Spy-Satellite Program*, WALL ST. J., June 23, 2009 (recounting congressional concerns that Posse Comitatus Act is violated by program that shares military satellite imagery with domestic agencies).

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.¹¹³

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. Federal law-enforcement and military personnel quickly cordoned off the town, and the two sides maintained an uneasy standoff for 71 days, occasionally exchanging gunfire. 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 to bring the standoff to a favorable outcome with minimum bloodshed.¹¹⁴ A number of the gunmen eventually found themselves in the dock facing a variety of federal criminal charges. 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,”¹¹⁵ because the military’s involvement at Wounded Knee violated the Posse Comitatus Act and thus rendered the officers’ actions unlawful.

Two judges agreed. *United States v. Jamarillo*¹¹⁶ held that the soldiers had so “perva[sively]” assisted the cops that there was a reasonable doubt whether the law-enforcement officers were lawfully engaged in the lawful performance of their duties.¹¹⁷ One of the things the *Jamarillo* court cited as an example of impermissible military involvement was giving tactical advice to law-enforcement officials – a form of information sharing.¹¹⁸ Similarly, in *United States v. Banks*,¹¹⁹ 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).¹²⁰ Two other judges saw things differently. *United States v. Red Feather*¹²¹ held that only the “direct active use” of soldiers to enforce the law violates the Posse Comitatus Act.¹²² Anything short of that – including the military’s behind-the-scenes assistance at Wounded Knee – is permissible. Likewise, *United States v. McArthur*¹²³ held that the information sharing and other forms of assistance didn’t offend the

¹¹³ See generally Canestaro, *supra* note 95, at 126 et seq.; Felicetti & Luce, *supra* note 92, at 145; Hohnsbeen, *supra* note 103, at 409-13.

¹¹⁴ See Hohnsbeen, *supra* note 103, at 409.

¹¹⁵ 18 U.S.C. § 231(a)(3).

¹¹⁶ 380 F. Supp. 1375 (D. Neb. 1974).

¹¹⁷ See *id.* at 1379.

¹¹⁸ See *id.* at 1381.

¹¹⁹ 383 F. Supp. 368 (D.S.D. 1974).

¹²⁰ See *id.* at 375, 376.

¹²¹ 392 F. Supp. 916 (D.S.D. 1975).

¹²² *Id.* at 923.

¹²³ 419 F. Supp. 186 (D.N.D.), *aff’d sub nom.* *United States v. Casper*, 541 F.2d 1275 (8th Cir. 1976), *cert. denied*, 430 U.S. 970 (1977).

Posse Comitatus Act, because the armed forces didn't subject citizens to military power that was "regulatory, proscriptive, or compulsory."¹²⁴

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 *Jamarillo* and *Banks*, that may well violate Posse Comitatus. Under *Red Feather* and *McArthur*, it probably doesn't. 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.¹²⁵

Of course, Congress is free to carve out exceptions to Posse Comitatus, and it has done so on a number of occasions.¹²⁶ The legality of information sharing is complicated by a 1981 exception intended to promote military cooperation with criminal investigations of narcotics trafficking in the Caribbean¹²⁷; 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."¹²⁸ 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.¹²⁹ The 1981 amendment thus reflects something like the "plain view" doctrine from Fourth Amendment law.¹³⁰ 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."¹³¹ 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 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'

¹²⁴ *Id.* at __.

¹²⁵ See *supra* note 49 and accompanying text.

¹²⁶ See, e.g., 10 U.S.C. § 332 (authorizing president to use armed forces to put down "unlawful obstructions, combinations, or assemblages, or rebellion against the United States," when it is "impracticable to enforce the laws of the United States in any state or territory by the ordinary course of judicial proceedings").

¹²⁷ See *Canestaro*, *supra* note 95, at 114; *Hohnsbeen*, *supra* note 103, at 417; *Kealy*, *supra* note 95, at 409; *Samek*, *supra* note 94, at 447; *Weber*, *supra* note 95, at 9.

¹²⁸ 10 U.S.C. § 371.

¹²⁹ 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 covering drug trafficking in the Caribbean." H.R. Rep. No. 87-71, at 8; see also *Hohnsbeen*, *supra* note 103, 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 FBI and DEA 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.

¹³⁰ See, e.g., *Arizona v. Hicks*, 480 U.S. 321 (1987).

¹³¹ 10 U.S.C. § 371.

intelligence activities may remove the resulting intelligence take from the murky category of “normal . . . military operations” and place it squarely in the realm of “otherwise . . . execut[ing] the laws.”

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 with domestic-intelligence functions. Roughly speaking, the bureau has two options for how to handle our hypothetical mall bombing: through a criminal investigation or an intelligence investigation. 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. 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”; 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 wouldn’t 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.¹³² In the immediate aftermath of the attack, it’s unlikely that the bureau will have decided whether to put the matter on the criminal track or the intelligence track. 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-variety crime or whether it’s 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 increases the likelihood that the armed forces will 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 armed forces it changes its mind 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 may well bar the retroactive imposition of criminal liability for data exchange that was lawful at the time it took place.)

Up to this point we’ve 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?

¹³² See *supra* note 85 and accompanying text.

This sort of transaction isn't 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."¹³³ The 1981 legislation thus may have something like an *expressio unis* effect, ruling out data exchange between the military and law enforcement that is not expressly authorized. 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 enforcement purposes 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.

D. 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. While the act sweepingly bars officials from disclosing covered records without the data subject's consent,¹³⁴ it's riddled with loopholes that give agencies fairly wide latitude to exchange data. Or so the story goes. In reality, the Privacy Act's exemptions aren't 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 collected¹³⁵ – 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.¹³⁶ 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. 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.¹³⁷

¹³³ 10 U.S.C. § 371 (emphasis added).

¹³⁴ 5 U.S.C. § 552a(b).

¹³⁵ See 5 U.S.C. § 552a(7).

¹³⁶ See *supra* notes 42 to 46 and accompanying text.

¹³⁷ See, e.g., S. REP. NO. 1183, 93d Cong., 2d Sess. ("[T]he creation of formal or de facto national data banks, or of centralized Federal information systems without certain statutory guarantees would . . . threaten . . . the values of privacy and confidentiality in the administrative process."); see also James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 35 (2003).

The Privacy Act addresses that concern in a number of concrete ways.¹³⁸ 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.”¹³⁹ Congress reportedly saw this nondisclosure requirement as “one of the most important, if not the most important, of the bill.”¹⁴⁰ The act contains a number of exceptions to its general prohibition on unconsented sharing of personal data, exceptions that are said to swallow the rule. By far the most important is the exemption that allows records to be shared for a “routine use.”¹⁴¹ 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”¹⁴²; second, the agency must publish a notice in the Federal Register.¹⁴³

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”¹⁴⁴ and “weak and ineffectual by today’s standards.”¹⁴⁵ And those are the favorable reviews. Others say the Privacy Act is either “a paper tiger,”¹⁴⁶ or “purely hortatory” and “entirely ineffective,”¹⁴⁷ or little more than “a procedural notice statute, rather than a safeguard against government invasion of individual privacy.”¹⁴⁸ There’s also widespread agreement that the act doesn’t prevent intelligence agencies from swapping data. The Markle Foundation’s task force on information policy and national security confidently predicted that “future government initiatives promoting increased interagency information sharing to protect national security will meet with little resistance” from the Privacy

¹³⁸ 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).

¹³⁹ 5 U.S.C. § 552a(b).

¹⁴⁰ H.R. REP. NO. 1416, 93d Cong., 2d Sess. 12 (1974); see also, e.g., BeVier, *supra* note 45, at 479 (describing nondisclosure requirement as “the heart of the Privacy Act”).

¹⁴¹ 5 U.S.C. § 552a(b)(3).

¹⁴² 5 U.S.C. § 552a(a)(7).

¹⁴³ 5 U.S.C. § 552a(3)(4)(D).

¹⁴⁴ Fred H. Cate, *Governing Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 465 (2008).

¹⁴⁵ Nehf, *supra* note 137, at 40.

¹⁴⁶ BeVier, *supra* note 45, at 479

¹⁴⁷ Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. Rev. 609, 633 (2007) [hereinafter Bignami, *Data Mining*].

¹⁴⁸ 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).

Act.¹⁴⁹ Academic commentators agree. “Certainly,” one article intones, “this allows all agencies involved in counterterrorism to share information.”¹⁵⁰

The Privacy Act’s exemptions may be fairly broad, but they don’t 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 regard compatibility as a significant hurdle. Routine use could prove a meaningful constraint on data exchange under this latter approach.¹⁵¹

The most restrictive readings come from the Third and Ninth Circuits. In *Britt v. Naval Investigative Service*,¹⁵² the defendant agency disclosed information about a Marine Corps reservist to his employer, the Immigration and Naturalization Service; 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.”¹⁵³ The court found the disclosure impermissible, holding that mere “[r]elevance” does not satisfy the routine use exemption’s compatibility requirement. “Congress limited interagency disclosures to more restrictive circumstances,” it explained. “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.”¹⁵⁴ 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. Postal Service*.¹⁵⁵ The plaintiff, a mail carrier in California, wrote letters to a Senator and Congressman alleging that her postmaster was deliberately undercounting rural mail routes. In response to inquiries from those officeholders, the Postal Service revealed that the plaintiff had filed a sex discrimination complaint with the EEOC. 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”).¹⁵⁶ Citing the Third Circuit’s ruling in *Britt*, the court emphasized that “compatibility requires more than mere relevance.”¹⁵⁷

¹⁴⁹ MARKLE FOUND., PROTECTING AMERICA’S FREEDOM IN THE INFORMATION AGE: A REPORT OF THE MARKLE FOUNDATION TASK FORCE 130 (2002) [hereinafter FIRST MARKLE REPORT].

¹⁵⁰ Dempsey & Flint, *supra* note 46, at 1475; *see also* BeVier, *supra* note 45, at 477; Bignami, *Transnational Intelligence*, *supra* note 45, at 672.

¹⁵¹ *See* BeVier, *supra* note 45, at 482-84; Cate, *supra* note 144, at 465; Coles, *supra* note 148, at 996-1000; FIRST MARKLE REPORT, *supra* note 149, at 129-30.

¹⁵² 886 F.2d 544 (3d Cir. 1989).

¹⁵³ *Id.* at 549.

¹⁵⁴ *Id.* at 549-50.

¹⁵⁵ 890 F.2d 1075 (9th Cir. 1989).

¹⁵⁶ *Id.* at 1078 (quoting 47 Fed. Reg. 1203 (1982)).

¹⁵⁷ *Id.* at 1078; *see also* Covert v. Harrington, 876 F.2d 751, 755 (9th Cir. 1989). There are some indications that Congress preferred a restrictive understanding of the compatibility requirement. 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

No so the D.C. Circuit, which takes a more flexible view of routine use. In *U.S. Postal Service v. National Association of Letter Carriers*,¹⁵⁸ 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. The court reasoned that, “in common usage, the word ‘compatible’ means simply ‘capable of existing together without discord or disharmony.’”¹⁵⁹ It therefore concluded that disclosures are only impermissible if they would undermine the agency’s reasons for collecting the data in the first place. “[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.”¹⁶⁰ 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.”¹⁶¹ For the D.C. Circuit, routine use isn’t much of a limit on interagency information sharing.¹⁶²

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 U.S. – e.g., the names of the crew, previous ports of call, the owners of the vessels, the owners of the cargo, and so on. 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. Suppose Customs wants to hand over its records to the National Security Agency. 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 it 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

fear that agencies would abuse it. The compromise was to retain the House’s routine use exemption while adding the compatibility requirement to limit agency discretion to transfer information. *See* Coles, *supra* note 148, at 976-78. Later, various members of Congress would reiterate their understanding that the compatibility requirement had some bite. *See, e.g.*, H.R. REP. NO. 927, 101st Cong., 2d Sess. 67 (1990):

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 absence of a sufficient nexus between those 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.

¹⁵⁸ 9 F.3d 138 (D.C. Cir. 1993).

¹⁵⁹ *Id.* at 144 (quoting WEBSTER’S THIRD NEW INT’L DICTIONARY 463 (1971)).

¹⁶⁰ *Id.*

¹⁶¹ *Id.* at 145.

¹⁶² The Office of Management and Budget – the agency that administers the Privacy Act – apparently has embraced the D.C. Circuit’s flexible 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. 52 Fed. Reg. 12,900, 12,993 (Apr. 20, 1987).

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 people¹⁶³; the two purposes aren’t “virtually identical.”¹⁶⁴

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. 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’s 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 penalties that can be assessed for disclosing records in violation of the Privacy Act. The act does not impose sanctions, criminal or otherwise, on individual officers who violate its terms. But it does allow a person injured by an unlawful disclosure to bring a civil action for money damages against the offending agency.¹⁶⁵ To be sure, the penalties are fairly modest. An offending agency is only on the hook for the “actual damages” sustained,¹⁶⁶ not punitive damages or any resulting emotional damages¹⁶⁷ – a far cry from the prospect of jail time under the Posse Comitatus Act. 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.¹⁶⁸

III. 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

¹⁶³ *Britt*, 886 F.2d at 549-50.

¹⁶⁴ *National Association of Letter Carriers*, 9 F.3d at 145.

¹⁶⁵ See 5 U.S.C. § 552a(g)(1)(D), (g)(4).

¹⁶⁶ 5 U.S.C. § 552a(g)(4)(A).

¹⁶⁷ See BeVier, *supra* note 45, at 481; Bignami, *Data Mining*, *supra* note 147, at 633; Coles, *supra* note 148, at 991-96.

¹⁶⁸ See *supra* note 49 and accompanying text.

unduly restricting information sharing? In general, yes to both. 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 entirely innocent information sharing. When considering how to accommodate these competing concerns, it will be useful to consult the insights of rational choice theory – the notion that government officials act to maximize their respective interests.¹⁶⁹ Looking beyond the four corners 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's unlikely that the CIA and 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. Similarly, sharing probably won't produce *firewall* harms under the 1947 act or the Posse Comitatus Act. Data exchange can actually vindicate firewall values by mitigating agencies' incentives to use aggressive intelligence and military techniques in inappropriate spheres. *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. 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.

A. Pretext Concerns

Like the Foreign Intelligence Surveillance Act, the National Security Act of 1947 – which prohibits CIA from exercising any “police, subpoena, or law enforcement powers” or performing any “internal security functions”¹⁷⁰ – 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. 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 collecting evidence for use in criminal proceedings; officials will fear that engaging in surveillance on behalf of their rival will enhance the FBI's welfare at the expense of their own. 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. In short, it isn't necessary to restrict data exchange between the FBI and CIA in an effort to prevent improper tasking, because the CIA's pursuit of its institutional interests typically will accomplish the same result.

¹⁶⁹ See, e.g., O'Connell, *supra* note 25 (developing rational choice framework to explain actions of intelligence agencies); Sales, *supra* note 9 (same); AMY B. ZEGART, SPYING BLIND 139 (2007) (same). See generally WILLIAM A. NISKANEN, JR., BUREAUCRACY AND REPRESENTATIVE GOVERNMENT (1971) (developing public choice account of administrative agency action); JAMES Q. WILSON, BUREAUCRACY (2d ed. 2000) (same).

¹⁷⁰ 50 U.S.C. § 403-4(d)(1).

Information sharing presents a risk that intelligence and law-enforcement agencies might 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 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 won't always be apparent whether a given sharing arrangement is innocuous or sinister. It's an evidentiary problem; data exchange that raises profound pretext problems will look quite similar to data exchange that is entirely innocent.

An information sharing wall between the FBI and 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,¹⁷¹ and 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.¹⁷² 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. CIA officials will want to treat the terrorist as an intelligence asset – question him to find out if he knows about plans to strike the U.S., try to turn him into a double agent who can be used to feed misinformation back to al Qaeda, and so on.

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 mount a criminal investigation will bolster the bureau's *influence* (its ability to persuade senior executive branch policymakers, such as the president, to accept its recommendations), as well as its *autonomy* (its ability to achieve its priorities without interference by outside entities).¹⁷³ 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

¹⁷¹ See generally MARK RIEBLING, WEDGE: FROM PEARL HARBOR TO 9/11: HOW THE SECRET WAR BETWEEN THE FBI AND CIA HAS ENDANGERED NATIONAL SECURITY (2002).

¹⁷² See POSNER, SURPRISE ATTACKS, *supra* note 1, at 29-31, 173-82.

¹⁷³ See Sales, *supra* note 9, at 304-13 (explaining that intelligence officials seek to maximize their agencies' influence and autonomy, and that such conduct can contribute to bureaucratic rivalries).

acute in cases where the target is a spy or terrorist who potentially could be dealt with either through law-enforcement tools or intelligence ones. 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"¹⁷⁴. The outer limits of what the National Security Act of 1947 proscribes may be ambiguous,¹⁷⁵ but running wiretaps for the express purpose of uncovering evidence to be used in criminal proceedings satisfies anybody's definition of "law enforcement." To be sure, the National Security Act of 1947 does not make CIA law enforcement activity a criminal offense. 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.¹⁷⁶ 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.¹⁷⁷

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,¹⁷⁸ but it's 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 investigators¹⁷⁹; FBI spies therefore may be more sympathetic to FBI cops' desire to collect evidence for criminal purposes than CIA spies would be.¹⁸⁰ The weaker that

¹⁷⁴ 50 U.S.C. § 403-4(d)(1).

¹⁷⁵ See *supra* notes 74 to 80 and accompanying text.

¹⁷⁶ See *supra* note 49 and accompanying text.

¹⁷⁷ 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 181 to 182. But the CIA's benefits are unlikely to outweigh its costs when the unlawful surveillance is undertaken at the FBI's behest.

¹⁷⁸ See sources cited *supra* note 67.

¹⁷⁹ See POSNER, UNCERTAIN SHIELD, *supra* note 16, at 98-99.

¹⁸⁰ *But cf.* WRIGHT, *supra* note 2, at 344, 352-54 (describing FBI criminal investigators' animosity for FBI intelligence operatives in the summer of 2001).

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 shouldn't lead us to inhibit information sharing between the FBI and CIA. Even if one rejects expanded coordination under FISA, it's still possible to embrace CIA-FBI data exchange to the extent it raises weaker pretext concerns.

B. Firewall Concerns

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. 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. 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 very 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 suspected al Qaeda operatives flying from Amsterdam to Detroit. 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. 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 doesn't 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 pressures to undertake domestic operations intended to gather the information it has no other way to obtain. Suppose CIA analysts know that a group of al Qaeda operatives has entered the country; the agency wants to listen to their phone calls and read their emails in the hopes of discovering whether they're about to mount 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'll 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 cafes they frequent.¹⁸¹

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. 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's 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 won't 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.

For reasons of institutional self interest and corporate culture,¹⁸² 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. 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.¹⁸³ 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 National Security Act of 1947 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. A military commander who directs his subordinates to engage in law enforcement functions, by contrast,

¹⁸¹ Cf. *Laird v. Tatum*, 408 U.S. 1 (1972).

¹⁸² Cf. ZEGART, *supra* note 169, at __ (using organizational theory to explain behavior of intelligence agencies); McNeal, 42 CASE W. RES. J. INT'L L. at 146 (same as to armed forces).

¹⁸³ See *supra* notes 98 to 99 and accompanying text.

may later be charged with violating the Posse Comitatus Act, a transgression that could land him in jail for up to two years.¹⁸⁴

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's 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 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.

C. 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. Second, Posse Comitatus helps keep the military from developing an institutional perspective on law-enforcement questions, thereby preserving independent domestic policy deliberations. 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. There's no doubt that 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's 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 isn't 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

¹⁸⁴ See 18 U.S.C. § 1385.

rebellious farmers in western Pennsylvania refused to pay. 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.¹⁸⁵ Yet when the crisis passed, the militias were deactivated without incident and civilian authorities suffered no enduring loss of power. 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.¹⁸⁶ Sometimes the army conducted the returns required by the act.¹⁸⁷ 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 schools¹⁸⁸; the army was implementing the requirements of the Supreme Court’s school-desegregation rulings.¹⁸⁹ 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’s 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 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 republican concerns. 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.¹⁹⁰ In short, the probability that data exchange will contribute to civilian authorities losing 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 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. 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.

¹⁸⁵ See generally ___.

¹⁸⁶ See generally ___.

¹⁸⁷ See, e.g., Tkacz, *supra* note 102, at 320-21.

¹⁸⁸ See generally ___.

¹⁸⁹ See, e.g., *Brown v. Board of Education*, 347 U.S. 483 (1954).

¹⁹⁰ See *supra* notes 181 to 184 and accompanying text.

The concern here 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 Founding¹⁹¹ – the ideal political decisionmaking process involves citizens reaching conclusions based on an independent, disinterested, and rational weighing of competing conceptions of the public good.¹⁹² 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. 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. In effect, citizens might delegate some of their responsibility for making informed policy judgments to the armed forces.

A lot can be said against this conception of political decisionmaking, including wondering (as liberal theorists do) whether it’s possible to conceive of a public good that is anything more than the sum of individual interests,¹⁹³ and questioning (as scholars of political ignorance do) whether citizens actually engage in the deliberations assumed by republican principles.¹⁹⁴ For our purposes, it’s 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 it’s to be expected that they will 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 the product of rational and independent deliberation that’s fully consistent with republican values. When deciding 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’s no reason to single out deference to the military as especially unwelcome.

¹⁹¹ See, e.g., Nathan Alexander Sales, *Classical Republicanism and the Fifth Amendment’s “Public Use” Requirement*, 49 DUKE L.J. 339, 349-50 (1999).

¹⁹² See, e.g., GORDON S. WOOD, *THE CREATION OF THE AMERICAN REPUBLIC* 55 (1969); MICHAEL J. SANDEL, *DEMOCRACY’S DISCONTENT* 5-6 (1996).

¹⁹³ See, e.g., Morton J. Horwitz, *Republicanism and Liberalism in American Constitutional Thought*, 29 WM. & MARY L. REV. 57, 68-69 (1987); SANDEL, *supra* note 192, at 7-8.

¹⁹⁴ See, e.g., ILYA SOMIN, *DEMOCRACY AND POLITICAL IGNORANCE* (forthcoming 2010).

Republicanism may or may not be offended by citizens deferring to the views of their churches, or 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, 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.

D. 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 avoiding government observation of personal facts; it expands the circle of officials who are privy to one’s private information. 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. Ultimately, privacy and information sharing are capable of peaceful coexistence; it’s 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.¹⁹⁵ That’s true, but it’s 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. When the FBI wiretaps a suspect’s phone, it won’t 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 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. By exposing investigators to these innocent and extraneous personal facts, surveillance can place severe strain on privacy values. (This is why FISA and Title III both require investigators to adopt “minimization” procedures – i.e.,

¹⁹⁵ See *supra* notes 42 to 46 and accompanying text.

procedures designed to reduce the amount of innocent content that's collected and to destroy what innocent content is gathered.¹⁹⁶⁾

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 don't share their raw surveillance take with one another – the innocent conversations along with the incriminating.¹⁹⁷ What are shared are the extracts – pieces of information that an analyst has processed, reviewed, and determined may be relevant to the investigation.¹⁹⁸ 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, where 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 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 email 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 emails, and the like?

¹⁹⁶ Compare 50 U.S.C. § 1801(h), with 18 U.S.C. § 2518(5).

¹⁹⁷ 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 16, at ____.

¹⁹⁸ See LOWENTHAL, *supra* note 16, at 55-67 (summarizing intelligence-production cycle).

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. 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 court¹⁹⁹ (and also helping the Justice Department’s Office of Intelligence Policy and Review shepherd that application through the FISA court’s approval process²⁰⁰). DHS officials will need to install and operate the taps; they may need to translate the overheard conversations and intercepted emails; 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 to the national security. 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.²⁰¹ In other words, the high cost of fresh surveillance will produce a substitution effect: Agency officials will switch to the lower-cost alternative of information sharing.²⁰²

It’s not 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.

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 won’t 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

¹⁹⁹ See 50 U.S.C. § 1804.

²⁰⁰ See 9/11 COMMISSION REPORT, *supra* note 2, at 78.

²⁰¹ 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. Some agencies are legally prohibited from engaging in various forms of domestic surveillance, such as CIA under the National Security Act of 1947 and the Army and Air Force under the Posse Comitatus Act. See *supra* Parts II.B, II.C. For these agencies, the costs of surveillance will include another consideration – the expected cost of breaking the law, or the magnitude of the harm associated with a statutory violation discounted by probability it will be detected. Because of these added costs, information sharing will tend to be even more attractive than fresh surveillance from standpoint of these agencies.

²⁰² Surveillance may be costly, but sharing can be costly, too. Perhaps the most important cost of sharing is the opportunity cost of foregone surveillance. 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.

surveillance. This is not to say that there are *no* privacy costs associated with information sharing; plainly there are.²⁰³ 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. 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 consent. 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. 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 isn’t 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. The intelligence community might make more extensive use of anonymization tools.²⁰⁴ Data that is to be shared with interagency partners (or even within a particular 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 depersonalized data, and would only need to learn individual identities if analysis turns up indications of possible terrorist

²⁰³ See *supra* notes 42 to 46 and accompanying text.

²⁰⁴ See, e.g., Don Clark, *Entrepreneur Offers Solution For Security-Privacy Clash*, WALL ST. J., Mar. 11, 2004.

activity.²⁰⁵ Or intelligence agencies could use immutable audit trails – i.e., computerized records that detail who has gained access to a particular piece of information.²⁰⁶ 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.” 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 notion that cops shouldn’t evade the legal limits on their surveillance powers by commissioning spies to do their dirty work for them, the notion that spies and soldiers should restrict their violent tradecraft to spheres where it belongs, the notion that civilian authorities must always be firmly in control of the armed forces, and the notion 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 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.

²⁰⁵ See MARKLE FOUND., CREATING A TRUSTED INFORMATION NETWORK FOR HOMELAND SECURITY: SECOND REPORT OF THE MARKLE FOUNDATION TASK FORCE 134, 144 (2003). *But see* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. __, __ (forthcoming 2010).

²⁰⁶ See, e.g., THIRD MARKLE REPORT, *supra* note 34, at 1-3, 6-7.