SMU | Dedman School of Law

SMU Law Review

Volume 60 | Issue 4 Article 9

January 2007

Counteracting Ambition: Applying Corporate Compliance and Ethics to the Separation of Powers Concerns with Domestic Surveillance

Paul E. McGreal

Recommended Citation

Paul E. McGreal, *Counteracting Ambition: Applying Corporate Compliance and Ethics to the Separation of Powers Concerns with Domestic Surveillance*, 60 SMU L. Rev. 1571 (2007)
https://scholar.smu.edu/smulr/vol60/iss4/9

This Essay is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in SMU Law Review by an authorized administrator of SMU Scholar. For more information, please visit http://digitalrepository.smu.edu.

COUNTERACTING AMBITION: APPLYING CORPORATE COMPLIANCE AND ETHICS TO THE SEPARATION OF POWERS CONCERNS WITH DOMESTIC SURVEILLANCE

*Paul E. McGreal**

INTRODUCTION

MY first political memory is from 1974, when I was seven years old. I remember seeing a man on television, and to my young mind, something did not look right. I asked my father who the man was and what he was doing. My dad said the man was going to be the new President: It was August 9, 1974, and Gerald Ford was taking the oath of office of the President of the United States. I remember asking what happened to the old President. My dad told me that the old President had done some bad things and so he had to give up his job. My memory fades at that point, but my guess is that I probably said "OK" and went back to playing with my baseball cards.

I begin with this story because it identifies an important point of reference: I came of age in the post-Watergate era, when limited and checked executive power was the norm, and suspicion—indeed, deep suspicion—of government officials was deemed the only prudent course. After all, this same era spawned the Office of the Independent Counsel,[1] a law barring bribery of foreign government officials,[2] and a law protecting the privacy of personal information held by the government.[3] The lesson was simple: When a government official says "trust me," it is best to do just the opposite.

This contrasts sharply with the view of some in the current administration. For example, Vice President Richard Cheney, who served in the

* Professor of Law, Southern Illinois University School of Law. This Essay extends my remarks delivered at the conference "Guarding the Guardians: The Ethics and Law of Domestic Surveillance," hosted by the Cary M. Maguire Center for Ethics and Professional Responsibility at Southern Methodist University on October 20, 2006. I thank my co-presenters for their comments and questions on my presentation. Also, special thanks to Professor Thomas Mayo, Director of the Maguire Center, for the invitation to participate in the event.

1. 28 U.S.C. § 591–599 (2005).
2. Foreign Corrupt Practices Act, 15 U.S.C. §§ 78dd-1 to -3, 78ff (2005).
3. Privacy Act, 5 U.S.C. § 552a (2005).

federal government during the pre- and post-Watergate era,[4] believes that Watergate swung the pendulum too far against executive power, artificially cabining the President.[5] Not surprisingly, this has led to rather broad claims of executive power, such as unilateral executive power to indefinitely detain and try foreign enemy combatants[6] and to conduct domestic surveillance,[7] as well as presidential signing statements that ignore disagreeable provisions of federal statutes.[8]

Going forward, the challenge is to balance suspicion of, and confidence in, executive power—to leave the executive flexibility to meet changing threats, while ensuring that flexibility is not a pretext for abuse. To begin answering this challenge, this Essay draws on expertise from an area of private law: the design, implementation, and operation of corporate compliance and ethics programs. A corporate compliance and ethics program consists of an organization's code of conduct, policies, and procedures that help achieve compliance with relevant laws as well as the organization's ethical standards.[9] My thesis is that constitutional separation of powers analysis ought to incorporate lessons from corporate compliance and ethics programs. Separation of powers requires adequate checks and balances to prevent abuse of federal power, and corporate compliance

4. Vice President Cheney served as President Ford's Chief of Staff. *See*, Vice President of the United States Richard B. Cheney, http://www.whitehouse.gov/vicepresident/ (last visited June 18, 2007).

5. *See* Michiko Kakutani, *The Case Against Those Expanding White House Powers*, N.Y. TIMES, July 6, 2007, at E32 ("[E]xpanded executive power was not a response to the terrorist attacks of 9/11 but the realization of a vision that conservatives like Dick Cheney had harbored since the 1970s, when they grew aggrieved over post-Watergate reforms that put the brakes on presidential power."); Tim Harper, *Cheney Argues for Nixon-Era Powers: Watergate Eroded Presidential Clout; VP Comments Fuel Firestorm in U.S.*, TORONTO STAR, Dec. 21, 2005, at A1 ("'Watergate and a lot of things around Watergate and Vietnam, both during the '70s served, I think, to erode the authority . . . the president needs to be effective, especially in the national security area,' Cheney told reporters aboard the Air Force Two aircraft after a visit to Pakistan."); Scott Shane, *Behind Power, One Principle*, N.Y. TIMES, Dec. 17, 2005, at A1 ("With the strong support of Vice President Dick Cheney, legal theorists in the White House and Justice Department have argued that previous presidents unjustifiably gave up some of the legitimate power of their office. The attacks of Sept. 11, 2001, made it especially critical that the full power of the executive be restored and exercised, they said."). Vice President Cheney had endorsed these same views in 1987 when, as representative of the State of Wyoming, he joined the Minority Report on the Iran-Contra Affair. *See* REPORT OF THE CONGRESSIONAL COMMITTEES INVESTIGATING THE IRAN-CONTRA AFFAIR, H.R. REP. NO. 100–433, at 457–58 (1987).

6. *See* Hamdi v. Rumsfeld, 542 U.S. 507, 535–36 (2004) (addressing the Administration's argument regarding detainees that "the courts must forgo any examination of the individual case and focus exclusively on the legality of the broader detention scheme").

7. *See* U.S. DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT (Jan. 19, 2006), *available at* http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf.

8. *See* AMERICAN BAR ASSOCIATION TASK FORCE ON PRESIDENTIAL SIGNING STATEMENTS AND THE SEPARATION OF POWERS DOCTRINE RECOMMENDATION 14–18 (2006), *available at* http://www.abanet.org/op/signingstatements/aba_final_signing_statements_recommendation-report_7-24-06.pdf (discussing second Bush administration's use of presidential signing statements).

9. For additional history and background on effective compliance programs, see generally Paul E. McGreal, *Legal Risk Assessment After the Amended Sentencing Guidelines: The Challenge for Small Organizations*, 23 CORP. COUNS. REV. 153 (2004).

and ethics programs have proven powerful checks on the abuse of corporate power. Corporate compliance and ethics best practices, then, can guide analysis of whether a given exercise of federal power incorporates adequate checks against abuse.

This Essay uses the example of domestic foreign intelligence surveillance to develop its thesis. In December 2005, the *New York Times* reported that the Bush Administration had conducted a form of domestic surveillance, known as the Terrorist Surveillance Program ("TSP"), for about three years:[10]

> Under a presidential order signed in 2002, the intelligence agency has monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people inside the United States without warrants over the past three years in an effort to track possible "dirty numbers" linked to Al Qaeda, the officials said. The agency, they said, still seeks warrants to monitor entirely domestic communications.[11]

Attorney General Alberto Gonzales later clarified the scope of the TSP:

> The President has authorized a program to engage in electronic surveillance of a particular kind, and this would be the intercepts of contents of communications where [. . .] one party to the communication is outside the United States. And this is a very important point—. . . one party to the communication has to be outside the United States. Another very important point to remember is that we have to have a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda. . . .
>
> What we're trying to do is learn of communications, back and forth, from within the United States to overseas with members of al Qaeda. And that's what this program is about.[12]

The Department of Justice claimed that both the President's inherent constitutional powers and federal law authorize such surveillance without judicial approval.[13] After a federal district court struck down the pro-

---

10. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

11. *Id.*

12. Press Briefing, Attorney General Alberto Gonzales & General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005), *available at* http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html. The Attorney General also explained that his remarks related only to the surveillance program already disclosed to the public:

> The President confirmed the existence of a highly classified program on Saturday. The program remains highly classified; there are many operational aspects of the program that have still not been disclosed and we want to protect that because those aspects of the program are very, very important to protect the national security of this country. So I'm only going to be talking about the legal underpinnings for what has been disclosed by the President.

Id.

13. While the Foreign Intelligence Surveillance Act (FISA) requires court approval for surveillance of communications where one party is within the United States, 50 U.S.C.

gram as violating separation of powers and the Fourth Amendment,[14] the Bush administration agreed to seek federal court approval for future surveillance.[15]

While the TSP is now defunct, it raises ongoing concerns regarding government power and personal liberty. This Essay applies its separation of powers thesis to these concerns: When the government conducts domestic surveillance, it should protect citizen privacy by designing and implementing a compliance and ethics program. Federal law already requires many private companies that collect customer data to do so, and this Essay simply proposes that the federal government take a dose of its own medicine.[16]

This Essay has five parts. Part I identifies the scope of the project. Part II reviews separation of powers first principles: Any program of domestic surveillance must satisfy these principles of checked and balanced power. Part III describes the current dilemma posed by counterterrorism: How to collect and analyze the mass of data needed to prevent the next terrorist attack while adequately protecting the privacy of United States citizens? Part IV describes how corporate compliance and ethics programs have allowed private companies to manage the risks posed by data privacy. Part V concludes by arguing that separation of powers analysis ought to ask whether the federal government has adopted similar compliance and ethics measures when handling data collected for surveillance purposes.

I. THE SCOPE OF THIS PROJECT

This Essay discusses the intersection of three subjects: domestic surveillance, separation of powers, and corporate compliance and ethics programs. The following sections briefly describe each topic.

---

§§ 1801– 1802 (2002), the Bush Administration has argued that Congress allowed such surveillance by passage of the Authorization for Use of Military Force, Pub. L. 107-40, 115 Stat. 224 (2001). *See* LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT, *supra* note 7, at 2–3. For a discussion of FISA's history and requirements, see ELIZABETH B. BAZAN, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: AN OVERVIEW OF THE STATUTORY FRAMEWORK AND U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT AND U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW DECISIONS (Congressional Research Service Feb. 15, 2007), *available at* http://www.fas.org/sgp/crs/intel/RL30465.pdf.

14. A.C.L.U. v. Nat'l Sec. Agency, 438 F. Supp. 2d 754, 782 (E.D. Mich. 2006), *rev'd on other grounds*, No. 06-2095, 2007 WL 1952370 (6th Cir. July 6, 2007).

15. Letter from Alberto R. Gonzales, U.S. Attorney Gen., to Hon. Patrick Leahy, Chairman, Comm. on the Judiciary, and Hon. Arlen Spector, Ranking Minority Member, Comm. on the Judiciary (Jan. 17, 2007), *available at* http://graphics8.nytimes.com/packages/pdf/politics/20060117gonzales_Letter.pdf.

16. As this Essay was in the editing process, the Department of Justice Announced that it was implementing additional internal controls over its national security activities. *See* Letter from Alberto R. Gonzales, U.S. Attorney Gen., to Hon. Richard B. Cheney, President of the Senate (July 13, 2007), *available at* http://www.justice.gov/opa/pr/2007/July/cheney_letter071307.pdf; Press Release, Fed. Bureau of Investigation, Justice Department and FBI Unveil Measures to Enhance National Security Oversight (July 13, 2007), *available at* http://www.justice.gov/opa/pr/2007/July/07_nsd_498.html.

A. DOMESTIC SURVEILLANCE

The intelligence challenge posed by terrorism can be stated rather simply: Predict where and when terrorists are likely to strike so the government can prevent future attacks. As will be discussed in Part III, counterterrorism's preventive focus means that government often starts without individualized suspicion, instead casting a wide intelligence net. This net will inevitably ensnare data of United States citizens for three main reasons. First, due to the nature of modern technology, even communications between individuals outside the United States may pass through and commingle with communications made solely within the United States.[17] Detection of such foreign communications necessarily requires surveillance of the commingled domestic communications. Second, some foreign terrorists, such as those who perpetrated the 9/11 attacks, plan and attack from within the United States. And third, some terrorist activity will be perpetrated by United States citizens, as was the

---

17. For example, e-mail messages travel in electronic packets that may take different paths to their destination:

> On the Internet, the network breaks an e-mail message into parts of a certain size in bytes. These are the packets. Each packet carries the information that will help it get to its destination—the sender's IP address, the intended receiver's IP address, something that tells the network how many packets this e-mail message has been broken into and the number of this particular packet. . . . Each packet contains part of the body of your message. A typical packet contains perhaps 1,000 or 1,500 bytes.
>
> Each packet is then sent off to its destination by the best available route—a route that might be taken by all the other packets in the message or by none of the other packets in the message. This makes the network more efficient. First, the network can balance the load across various pieces of equipment on a millisecond-by-millisecond basis. Second, if there is a problem with one piece of equipment in the network while a message is being transferred, packets can be routed around the problem, ensuring the delivery of the entire message.

How Stuff Works, "What Is a Packet?", http://www.howstuffworks.com/question525.htm (last visited July 30, 2007). Surveillance for e-mail messages, then, must monitor the various routes a message may take and electronically "sniff" all the packets as they move through. Not surprisingly, this process is known as "packet sniffing":

> Essentially, a packet sniffer is a program that can see all of the information passing over the network it is connected to. As data streams back and forth on the network, the program looks at, or "sniffs," each packet.
>
> Normally, a computer only looks at packets addressed to it and ignores the rest of the traffic on the network. When a packet sniffer is set up on a computer, the sniffer's network interface is set to promiscuous mode. This means that it is looking at everything that comes through. The amount of traffic largely depends on the location of the computer in the network. A client system out on an isolated branch of the network sees only a small segment of the network traffic, while the main domain server sees almost all of it.
>
> A packet sniffer can usually be set up in one of two ways:
>
> Unfiltered - Captures all of the packets
>
> Filtered - Captures only those packets containing specific data elements
>
> Packets that contain targeted data are copied as they pass through. The program stores the copies in memory or on a hard drive, depending on the program's configuration. These copies can then be analyzed carefully for specific information or patterns.

How Stuff Works "How Carnivore Worked", Packet Sniffing, http://computer.howstuffworks.com/carnivore2.htm (last visited July 30, 2007).

attack on the federal courthouse in Oklahoma City. In short, some domestic surveillance is inherent in effective counterterrorism efforts.

B. Separation of Powers (and Not the Fourth Amendment)

This Essay focuses on the separation of powers concerns raised by domestic surveillance, leaving aside the question whether such surveillance violates the Fourth Amendment search and seizure provisions.[18] This focus, however, does not ignore values and principles central to the Fourth Amendment. For one, separation of powers itself protects individual liberty, as each branch of government is supposed to check abuses of power by the other. Indeed, as the Court recently reiterated in *Hamdi v. Rumsfeld*,[19] it is when government action threatens individual liberty that strong checks are needed the most.[20]

Second, the Fourth Amendment incorporates notions of procedural checks on abuse of power. For example, the Supreme Court has allowed state police to conduct roadblocks to detect drunk drivers and protect roadway safety.[21] Such roadblocks burden the privacy protected by the Fourth Amendment by subjecting some travelers to unwanted scrutiny by law enforcement. Further, the roadway stops pose the threat that law enforcement will either discriminatorily target drivers based on a forbidden ground (for example, race, gender, etc.), or that the stops are a pretext for detecting other crimes (for example, drug or firearm possession). The Court has permitted roadblocks only when procedural safeguards reduce the risk of police abuse.[22]

C. Corporate Compliance and Ethics Programs

A company's compliance and ethics program consists of the personnel, policies, and procedures that ensure employees and agents adhere to the company's legal and ethical obligations.[23] For example, if a company has agents that do business overseas, it must address the risk that those agents might bribe foreign government officials to obtain business.[24] The company should draft policies addressing payments to foreign government officials, train its agents on the relevant policies, monitor and audit

18. U.S. Const. amend. IV; *see ACLU*, 438 F. Supp. 2d at 773–75 (reviewing the constitutionality of the TSP under the Fourth Amendment).

19. 542 U.S. 507, 535–36 (2004).

20. *Id.* at 536.

21. *See* Illinois v. Lidster, 540 U.S. 419, 421–22 (2004) (upholding drunk driving arrest made at a checkpoint established to ask motorists about recent hit-an-run accident in the area); Indianapolis v. Edmond, 531 U.S. 32, 47–48 (2000); Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 455 (1990).

22. *Lidster*, 540 U.S. at 428 ("The police stopped all vehicles systematically. And there is no allegation here that the police acted in a discriminatory or otherwise unlawful manner while questioning motorists during stops.") (citations omitted).

23. For a more detailed discussion of the origin, nature, and extent of corporate compliance programs, see Paul McGreal, *Corporate Compliance Survey*, 61 Bus. Law. 1645 (2006).

24. *See* Foreign Corrupt Practices Act of 1977, 15 U.S.C. §§ 78dd-1 to -3, 78m, 78ff (2000).

its agents' expense statements, investigate suspicious activity, and discipline those who violate the policy. As Part IV explains, a rich literature discusses the best practices for designing and implementing each step of a corporate compliance and ethics program.

II. SEPARATION OF POWERS FIRST PRINCIPLES

Part II is *not* a summary or exposition of separation of powers doctrine.[25] Rather, this Essay returns to the constitutional foundation, identifying first principles that underlie separation of powers analysis. The discussion does so through a series of quotes that capture the main points. The first three quotes are from James Madison's contributions to *The Federalist Papers*;[26] the next two quotes are from the Supreme Court's 2004 detainee decision in *Hamdi v. Rumsfeld*;[27] and the last two quotes are from Justice Robert Jackson's canonical concurrence in *Youngstown Sheet & Tube Co. v. Sawyer*.[28] Each quote is followed by observations about separating power among the three branches of the federal government.

"IF MEN WERE ANGELS, NO GOVERNMENT WOULD BE NECESSARY."[29]

This truism is the root of all other separation of powers principles. Whether due to self-interest, prejudice, or some other human failing, society requires an organizing force to ensure order.[30] And this principle applies to the rulers as well as the ruled, for a "government of the people, by the people, and for the people"[31] will necessarily be "the greatest of all reflections on human nature."[32] Consequently, "[i]n framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself."[33] This is an application of Lord Acton's Dictum: "Power tends to corrupt; absolute power corrupts absolutely."[34] The question is how best to get the government to "control itself."

---

25. As the war on terror has been waged, this topic has been discussed at length. *See, e.g.*, Neal Kumar Katyal, *Toward Internal Separation of Powers*, 116 YALE L.J. POCKET PART 106 (2006); Michael D. Ramsey, *Textualism and War Powers*, 69 U. CHI. L. REV. 1543 (2002); Mark Tushnet, *Controlling Executive Power in the War on Terrorism*, 118 HARV. L. REV. 2673 (2005).

26. THE FEDERALIST NO. 51 (James Madison).

27. 542 U.S. 507 (2004).

28. 343 U.S. 579 (1952).

29. THE FEDERALIST NO. 51 (James Madison).

30. 1 FRIEDRICH A. HAYEK, LAW, LEGISLATION AND LIBERTY: A NEW STATEMENT OF THE LIBERAL PRINCIPLES OF JUSTICE AND POLITICAL ECONOMY: RULES AND ORDER 72 (1973) ("Law in the sense of enforced rules of conduct is undoubtedly coeval with society; only the observance of common rules makes the peaceful existence of individuals within society possible.").

31. Abraham Lincoln, U.S. President, the Gettysburg Address (Nov. 19, 1863).

32. THE FEDERALIST NO. 51 (James Madison).

33. *Id.*

34. Letter from John Dahlberg-Acton to Bishop Mandell Creighton (Apr. 1887) (*reprinted in* THE NEW DICTIONARY OF CULTURAL LITERACY (E.D. Hirsch, Jr., Joseph F.

"AMBITION MUST BE MADE TO COUNTERACT AMBITION."[35]

This quote begins to answer how government might control the rulers—a form of intra-governmental divide and conquer. Later in the same passage, Madison elaborates on his point:

> [T]he great security against a gradual concentration of the several powers in the same department, consists in giving to those who administer each department the necessary constitutional *means* and personal *motives* to resist encroachments of the others. The provision for defense must in this, as in all other cases, be made commensurate to the danger of attack. . . . . This policy of supplying, by opposite and rival interests, the defect of better motives, might be traced through the whole system of human affairs, private as well as public. We see it particularly displayed in all the subordinate distributions of power, where the constant aim is to divide and arrange the several offices in such a manner as that each may be a *check* on the other that the private interest of every individual may be a sentinel over the public rights.[36]

In short, government ought to be self-policing, and this plan had three parts. First, while "dependence on the people" for re-election will be the "primary control" against tyranny, an essential "auxiliary precaution" is for each branch to check abuses of power by the other branches.[37] Hence the description of American government as one of checks and balances. Second, an effective system of checks requires that each branch have adequate "means"—that is, power—to check the other branches. For example, the executive can check legislative overreaching through the veto[38] and the exercise of prosecutorial discretion.[39] The legislature can check executive ambition by overriding a presidential veto,[40] controlling federal spending,[41] or impeaching executive officials.[42] Third, each branch must be given the "motive"—that is, an incentive—to use their powers to check the other branches.[43]

"THE ACCUMULATION OF ALL POWERS, LEGISLATIVE, EXECUTIVE, AND JUDICIARY, IN THE SAME HANDS . . . MAY JUSTLY BE PRONOUNCED THE VERY DEFINITION OF TYRANNY."[44]

This quote is a corollary of the preceding one: If all power is consolidated in the hands of a single branch, no other branch can check that

---

Kett, & James Trefil eds.) (3rd ed. 2002) (referring to the doctrine of papal infallibility in the Catholic Church)).

35. THE FEDERALIST NO. 51 (James Madison).
36. *Id.* (emphasis added).
37. *Id.*
38. U.S. CONST. art. I, § 7, cl. 2.
39. *Id.* art. II, § 3 (the President "shall take care that the laws be faithfully executed").
40. *Id.* art. I, § 7, cl. 2.
41. *Id.* art. I, § 7, cl. 1.
42. *Id.* art. I, § 2, cl. 5; § 3, cl. 6–7.
43. Paul E. McGreal, *Ambition's Playground*, 68 FORDHAM L. REV. 1107, 1140-41 (2000).
44. THE FEDERALIST NO. 47 (James Madison).

branch's ambition. Without checks, we are back to absolute power and so tyranny. Yet, the danger of all government power ending up in the hands of a single branch is relatively small. The real threat is unchecked power over a specific subject, such as the treatment of those designated as unlawful enemy combatants.[45] While limited in scope, such power would be tyranny nonetheless.[46] So, this adage not only warns against collapsing government into a single branch, but urges vigilance against pockets of unchecked government power.

"[A] STATE OF WAR IS NOT A BLANK CHECK FOR THE PRESIDENT WHEN IT COMES TO THE RIGHTS OF THE NATION'S CITIZENS."[47]

This principle anticipates a specific argument for consolidated federal power: "But we are at war!" Of course, war may provide a rationale for government action, or even justify deference to executive decisions.[48] But war does not override the basic principle that each branch of government has limited, checked power.

"[T]HE UNITED STATES CONSTITUTION . . . MOST ASSUREDLY ENVISIONS A ROLE FOR ALL THREE BRANCHES WHEN INDIVIDUAL LIBERTIES ARE AT STAKE."[49]

This principle is a further corollary of the warning against consolidating government power. The President and Congress rarely claim sole power over a particular subject, but instead argue for great deference from the judicial branch. At times, this deference asks federal courts to simply accept, without scrutiny, a judgment of that branch. For example, the President has argued that federal courts should accept the executive's sole judgment as to whether a person is an unlawful enemy combatant subject to trial before a military commission.[50]

Generally speaking, arguments for judicial deference are appropriate, as the judiciary must guard against accumulating too much power within its own hands (that is, tyranny of the judiciary). The case for deference, however, is weakest when individual liberties are at stake. Claims of individual liberties often arise in cases where an unpopular individual opposes the will of the popular branches of government, making protection in the political process unlikely. The federal judiciary, insulated from popular pressure by life tenure,[51] is better situated to defend the rights of these unpopular individuals. Thus, the federal courts should carefully

45. Hamdan v. Rumsfeld, 126 S. Ct. 2749, 2780 (2006).

46. *See* Clinton v. City of New York, 524 U.S. 417, 450 (1998) (Kennedy, J., concurring) (striking down the Line Item Veto Act as a violation of separation of powers).

47. Hamdi v. Rumsfeld, 542 U.S. 507, 536 (2004).

48. *See generally* WILLIAM H. REHNQUIST, ALL THE LAWS BUT ONE: CIVIL LIBERTIES IN WARTIME (1998).

49. *Hamdi*, 542 U.S. at 536.

50. *Id.* at 535–36.

51. U.S. CONST. art. III, § 1 ("The Judges, both of the supreme and inferior Courts, shall hold their Offices during good Behaviour").

scrutinize arguments for judicial deference when individual liberties are at stake.

"[THE FRAMERS] SUSPECTED THAT EMERGENCY POWERS WOULD TEND TO KINDLE EMERGENCIES."[52]

This principle is a specific application of the insight that government actors tend to seek expansion of their power. In *Youngstown Sheet & Tube Co. v. Sawyer*,[53] decided during the Korean War, President Truman argued that the Supreme Court ought to recognize implied emergency powers in the executive branch. Justice Jackson's concurring opinion noted that any such power was likely to expand with the imagination of whomever held the office.[54] A President faced with no enumerated power to justify an action would simply declare an emergency.[55] Justice Jackson's core insight is that federal courts ought to precisely and carefully define executive power, as the future tendency will be toward the most expansive application of that power.[56]

"WHILE THE CONSTITUTION DIFFUSES POWER THE BETTER TO SECURE LIBERTY, IT ALSO CONTEMPLATES THAT PRACTICE WILL INTEGRATE THE DISPERSED POWERS INTO A WORKABLE GOVERNMENT."[57]

This last principle is itself a check on the preceding principles: Checks on government power ought not paralyze the government. The federal courts must be sensitive to the practical consequences of their doctrines. We want a government of checks *and balances*, with judicial review striking a realistic, workable balance. For, as President Abraham Lincoln asked, "Was it possible to lose the nation, and yet preserve the constitution?"[58]

III. THE THREAT TO LIBERTY FROM DOMESTIC SURVEILLANCE

Several commentators have noted that combating terrorism requires a different focus from conventional law enforcement.[59] While law enforcement takes a completed or ongoing action and asks who did it, counterterrorism makes a predictive judgment to identify terrorists *before* they strike. To quote the 9/11 Commission, "terrorism cannot be

52. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 650 (1952) (Jackson, J., concurring in the judgment).
53. *Id.* at 587.
54. *See id.* at 634–38.
55. *Id.*
56. *Id.*
57. *Id.* at 635.
58. Letter from Abraham Lincoln, President, United States, to Albert G. Hodges, Editor, Commonwealth (Frankfort, KY) (Apr. 4, 1864) (*available at* http://memory.loc.gov/ammem/alhtml/almss/ln001.html).
59. *See generally* RICHARD A. POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY (2006) [hereinafter POSNER, SUICIDE PACT].

treated as a reactive law enforcement issue, in which we wait until after the bad guys pull the trigger before we stop them."[60]

Judge Richard Posner notes that this shift from law enforcement to counterterrorism enlarges the amount of data required by the government:

> [P]revention requires intelligence agencies to cast a much wider and finer-meshed net in fishing for information. Once a crime has occurred, a focused search for the criminal and for evidence of the crime is feasible. But if the concern guiding a search is that a crime might occur, the focus has to be much broader.[61]

This change makes probable cause and reasonable suspicion—traditional triggers for searches and seizures for domestic law enforcement—problematic.[62] For requiring individualized suspicion, the argument goes, misses the very point of counterterrorism surveillance: We do not know who they are or what they are planning.[63]

To illustrate the breadth of counterterrorism surveillance, consider the example of data-mining:[64]

> Data mining is the process of looking for new knowledge in existing data. The basic problem addressed by data mining is turning low-level data, usually too voluminous to understand, into higher forms (information or knowledge) that might be more compact (for example, a summary), more abstract (for example, a descriptive model), or more useful (for example, a predictive model). At the core of the data mining process is the application of data analysis and discovery algorithms to enumerate and extract patterns from data in a database.[65]

---

60. Editorial, *The Limits of Hindsight*, WALL ST. J., July 28, 2003, at A10; *see also* POSNER, SUICIDE PACT, *supra* note 59, at 92–93 ("[W]hen the government is fighting terrorism rather than ordinary crime, the emphasis shifts from punishment to prevention.").

61. POSNER, SUICIDE PACT, *supra* note 59, at 92–93.

62. *See* Richard A. Posner, *A New Surveillance Act*, WALL ST. J., Feb. 15, 2006, at A16 ("[The Foreign Intelligance Surveillance Act] retains value as a framework for monitoring the communications of known terrorists, but it is hopeless as a framework for detecting terrorists. [FISA] requires that surveillance be conducted pursuant to warrants based on probable cause to believe that the target of surveillance is a terrorist, when the desperate need is to find out who is a terrorist.").

63. K. A. Taipale, *Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd*, 7 YALE J. L. & TECH. 123, 176–83 (2005).

64. For a skeptical view of whether data mining's proponents has proven that method's efficacy, see Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 74 U. CHI. L. REV. (forthcoming 2007), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=990030. The Associated Press has reported that the Federal Bureau of Investigation is planning a large-scale data mining project. Michael J. Sniffen, *FBI Plans Huge Anti-Terror Data-Mining*, ASSOCIATED PRESS, June 12, 2007.

65. K. A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 2, 21 (2003); *see also* U.S. GEN. ACCOUNTING OFFICE, GAO-04-548, DATA MINING: FEDERAL EFFORTS COVER A WIDE RANGE OF USES 1 (2004), *available at* http://www.gao.gov/new.items/d04548.pdf ("The term 'data mining' has a number of meanings. For purposes of this work, we define data mining as the application of database technology and techniques—such as statistical analysis and model-

Judge Posner describes the types of searches data mining might include:

> Because of the volume involved, massive amounts of intercepted data must first be sifted by computers. The sifting can take two forms. One is a search for suspicious patterns or links; [for example,] searching for "use of a stolen credit card for a small purchase at a gas station—done to confirm whether a card is valid—before making a very significant purchase," a pattern suggestive of credit card fraud. The other form is the familiar Google-type search for more information about a known individual, group, subject, activity, identifier, and so on. A search for a social security number, for example, can reveal whether two similar or identical names are the names of two persons or one. The term "data mining" is sometimes limited to the first, the pattern search. But it is often used to embrace the second as well.[66]

While ordinary law enforcement begins with a known criminal act, and so might search a database by querying fields (such as name, address, social security number) for known information, counterterrorism tries to prevent unknown events by unknown perpetrators, which makes the entire database potentially relevant.[67] The challenge in data mining is to analyze the underlying data using technologies that can reveal patterns and relationships that would otherwise go undetected.

To perform data mining, the government must identify, collect, and aggregate data, as do innumerable private firms that handle customer data:

> Because terrorist groups and affiliations are now global, because the number of potential terrorist targets is almost unlimited, because the variety of weaponry to which these groups may gain access is enormous, because modern surveillance technology can vacuum vast amounts of data, and because some terrorist groups are good at biding their time—which means that data from years ago may shed light on current and future terrorist schemes—the quantity of collectible data that may contain clues to terrorist plans or activities is immense, though not necessarily more immense than the data that commercial

---

ing—to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results.") [hereinafter GAO DATA MINING REPORT].

66. POSNER, SUICIDE PACT, *supra* note 59, at 96–97 (2006).

67. The Government Accounting Office describes one such data-mining effort:

> One example of a large-scale development effort launched in the wake of the September 11 attacks is the Multistate Anti-terrorism Information Exchange System, known as MATRIX. MATRIX, currently used in five states, provides the capability to store, analyze, and exchange sensitive terrorism-related and other criminal intelligence data among agencies within a state, among states, and between state and federal agencies. Information in MATRIX databases includes criminal history records, driver's license data, vehicle registration records, incarceration records, and digitized photographs. Public awareness of MATRIX and of similar large-scale data mining or data mining-like projects has led to concerns about the government's use of data mining to conduct a mass "dataveillance"—a surveillance of large groups of people—to sift through vast amounts of personally identifying data to find individuals who might fit a terrorist profile.

GAO DATA MINING REPORT, *supra* note 65, at 5.

services handle more or less effortlessly.[68]

Similarly, private firms routinely analyze such data:

> To be assembled, retrieved, sorted, and sifted, so that patterns can be discerned and inferences drawn, intelligence data must be digitized, and the digitized data organized in databases linked to thousands of workstations (terminals, laptops, cellphones, in-vehicle displays, etc.) scattered throughout the intelligence system, not to mention tens of thousands of workstations elsewhere in the nation's farflung, poorly integrated, federal, state, local, and private security network. But that too is not unique.[69]

And like data collected by private firms, the government's data will be vulnerable to abuse or attack.[70] Data could be improperly disclosed, either through inadvertence or misconduct of government personnel who handle the data, or through the wrongful acts of those who obtain unauthorized access to the data.[71] Disclosure can cause harm through either embarrassment or the subsequent misuse of the information (for example, identity theft or blackmail).[72] Also, the data could be abused by those with authorized access,[73] as when the government targets its political opponents.[74] And even legitimate use of the data can lead to false positives, such as when an innocent person is mistakenly identified as a terrorist target.[75]

The threats posed by domestic surveillance raise serious separation of powers concerns. Recall that when liberty is at issue,[76] first principles counsel that the federal courts should play some role in checking abuses of government power. Here, the judiciary must play some role checking

---

68. RICHARD A. POSNER, UNCERTAIN SHIELD: THE U.S. INTELLIGENCE SYSTEM IN THE THROES OF REFORM 141 (Peter Berkowitz & Tod Lindberg eds. 2006) [hereinafter POSNER, UNCERTAIN SHIELD].

69. *Id.* at 141–42.

70. POSNER, SUICIDE PACT, *supra* note 59, at 97–98 ("The principal worry about these searches from the standpoint of privacy, besides fear that hackers will gain access to the contents of the intercepted communications, is that those contents might be used to blackmail or otherwise intimidate the administration's critics and political opponents. A secondary fear is that they might be used to ridicule or embarrass. Such things have happened in the past, but they are less likely to happen today."). For a thorough discussion of the various aspects of privacy, as well as its specific application to surveillance, see Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

71. The Privacy Act provides, in part, 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. . . ." 5 U.S.C. § 552a(b) (2005).

72. *See* Solove, *supra* note 70, at 536, 542.

73. *See* Taipale, *supra* note 63, at 176–83; Press Release, U.S. Dep't of Justice, FBI Legal Technician Pleads Guilty To Unlawfully Accessing The FBI's Computer System (Feb. 26, 2004) *available at* http://www.usdoj.gov:80/opa/pr/2004/February/04_crm_120.htm.

74. COMM'N ON CIA ACTIVITIES WITHIN THE UNITED STATES, REPORT TO THE PRESIDENT 172–207 (June 1975).

75. *See* Solove, *supra* note 70, at 516-19.

76. POSNER, UNCERTAIN SHIELD, *supra* note 68, at 87–88 ("Domestic intelligence presents civil liberties concerns that are absent when intelligence agencies operate abroad, since the Constitution and laws of the United States do not have extra-territorial application.").

the abuses posed by data collection, analysis, and storage. Part V argues that judicial review ought to examine whether the government's domestic surveillance programs implement an effective compliance and ethics program designed to reduce threats to data security. The next part describes what such a program entails.

IV. COMPLIANCE AND DATA PRIVACY

This Part links compliance and ethics programs to constitutional law. Section A describes the elements of an effective compliance and ethics program. Section B then explains how the 1977 case, *Whalen v. Roe*[77] incorporated the concept of compliance and ethics into its constitutional analysis of database privacy. Section C then describes how modern federal law has developed concrete guidance for designing and implementing an effective data privacy compliance and ethics program.

A. COMPLIANCE GENERALLY

All businesses take some measures to ensure that their employees and agents comply with applicable laws. After all, the simple directive to "be careful" is an informal attempt to comply with the negligence duty of care. Compliance and ethics programs formalize and expand upon these ad hoc efforts. The formality comes from designating personnel responsible for the compliance and ethics programs, and implementing organizational infrastructures that carry out the various compliance and ethics functions. The expansion comes from a comprehensive attempt to identify and address the organization's legal risks and ethical principles.

Historically, businesses have had two main reasons to implement a compliance and ethics program. First, such programs hold the promise of reducing misconduct by both educating employees about their legal responsibilities and deterring potential wrongdoers.[78] Compliance and ethics programs, then, are sensible when the expected reduction in liability costs exceeds the cost of implementing the program.[79] Second, after prosecuting an organization for wrongdoing, the government has often required implementation of a compliance and ethics program.[80] This oc-

77. 429 U.S. 589 (1976).

78. Generally, corporate compliance and ethics programs are not a defense to corporate criminal or civil vicarious liability. *See generally* Andrew Weissmann with David Newman, *Rethinking Criminal Corporate Liability*, 82 IND. L.J. 411 (2007). There are, however, specific regulatory areas where the government has incentivized the institution of such programs. *See infra* notes 80–86 and accompanying text.

79. Costs would include not only the pecuniary payout for liability (for example, fines, damages), but also the costs of dealing with the claim of legal violation (for example, attorneys fees, opportunity cost of responding to the claims), loss of good will, and other similar costs associated liability.

80. *See* Weissmann with Newman, *supra* note 78, at 444–46 (discussing the Department of Justice's use of deferred prosecution agreements). The government has also recently included compliance requirements in corporate deferred prosecution agreements. *See* Brandon L. Garrett, *Structural Reform Prosecution*, 93 VA. L. REV. 853, 904 (2007).

curred after industry scandals involving price fixing, insider trading, and health care fraud.

Over the last fifteen years, the incentives towards compliance have themselves become more formal. The trend began in 1991 when the United States Sentencing Commission promulgated organizational sentencing guidelines that mandated leniency for organizations that had an effective compliance and ethics program.[81] Since then, a variety of state and federal agencies have encouraged compliance and ethics programs through guidance or incentives. For example, the Office of the Inspector General in the United States Department of Health and Human Services has issued compliance program guidance for preventing health care fraud,[82] and the United States Department of Justice has directed United States Attorneys to consider either deferring or declining prosecution of organizations that have an effective compliance and ethics program.[83] In addition, an effective program can defend against vicarious civil liability for sexual harassment,[84] commodities fraud,[85] or workplace safety violations.[86] And a recent wave of laws and regulations *require* compliance and ethics programs, making the program *itself* an aspect of complying with the law.[87] The clear legal trend is toward greater emphasis on private compliance and ethics programs.

While compliance and ethics programs cover a variety of risks and industries, they contain a basic set of elements regardless of the organization. The following ten steps are core requirements of an effective program:[88]

1. Periodic risk assessments

---

81. Amendments to the Sentencing Guidelines for United States Courts, 56 Fed. Reg. 22,762 (May 16, 1991) (amending U.S. SENTENCING GUIDELINES MANUAL § 8C2.5(f).

82. *See* McGreal, *supra* note 23, at n.43-52 (discussing the HHS compliance guidance documents).

83. Memorandum from Paul J. McNulty, Deputy Attorney Gen., to Heads of Dep't Components and United States Attorneys 12-15 (Dec. 12, 2006), *available at* http://www.corporatecompliance.com/events/07docs/AC-McNulty/FTL1-20075Lv/Paul%205.pdf.

84. *See* McGreal, *supra* note 23, at n.76-68.

85. *See* Commodity Futures Trading Comm'n v. Carnegie Trading Group, Ltd., 450 F. Supp. 2d 788, 804–05 (N.D. Ohio 2006).

86. *See* W.G. Yates & Sons Constr. Co. v. Occupational Safety & Health Review Comm'n, 459 F.3d 604, 608–09 (5th Cir. 2006).

87. For example, the USA Patriot Act requires financial institutions to implement and operate anti-money laundering compliance programs, with the failure to do so subjecting the firm to a fine. 31 U.S.C.A. § 5318(h) (West 2002). And three states now require organizations with more than fifty employees to provide biennial sexual harassment training for supervisors. *See* CAL. GOV'T CODE ANN. § 12950.1 (West Supp. 2006); CONN. GEN. STAT. ANN. § 46a-54(15)(B) (West Supp. 2006); MAINE REV. STAT. ANN. tit. 26, § 807(3) (Supp. 2006). Some state statutes merely "encourage" employers to provide such training. *See, e.g.*, VT. STAT. ANN. tit. 21, § 495h(f) (2003) ("Employers . . . are encouraged to conduct an education and training program . . . for all current employees . . . and for all new employees . . . .").

88. Depending on the author, the precise number of steps may vary, but the core components will be the same. For example, the current United States Sentencing Guidelines list eight steps, as they include the code of conduct and drafting of written compliance standards into a single step. *See* U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b) (2006), *available at* http://www.ussc.gov/2006guid/8b2_1.html.

2. Involvement of the organization's governing authority
3. Designating compliance personnel
4. Code of conduct
5. Written compliance and ethics standards and procedures
6. Employee and agent training
7. Lines of communication
8. Auditing and monitoring
9. Enforcement, discipline, and positive incentives
10. Periodic evaluation and improvement

Consider each step in turn.

1. *Periodic risk assessments*: The organization must identify and prioritize its legal and other risks. Once completed, the risk assessment serves as the blueprint for designing and operating the compliance and ethics program. A risk assessment should be performed both when designing a program and at sensible intervals thereafter.[89]

2. *Involvement of the organization's governing authority*: The organization's board (or other similar body) should initiate and exercise oversight of the compliance and ethics program. This typically entails authorizing resources and personnel to undertake the compliance effort, and establishing a timetable and measurable goals. Thereafter, the board should exercise oversight through regular reports from compliance personnel. Along with upper management, the board sets the "tone at the top," showing that the organization takes its compliance and ethics program seriously.

3. *Designating compliance personnel*: The organization must assign someone overall responsibility for the compliance and ethics program, and assign someone else responsibility for day-to-day operation of the program. Typically, overall responsibility resides in a chief compliance officer. The main concern here is that the chief compliance officer have the time, authority, and resources to carry out the compliance functions. For example, an organization should consider carefully whether to add the chief compliance officer title to the general counsel, who may already wear several other hats within the organization.[90]

4. *Code of conduct*: The code of conduct is the constitution of the compliance and ethics program. As such, the code should set forth the program's broad outlines, leaving the details for specific policies. The code should summarize the organization's core values, identify its major legal risks, identify the personnel responsible for the program's components, and describe the processes for asking questions and reporting violations. Further, the code should be written so that it is relevant and accessible to the organization's various constituencies.[91]

89. *See* McGreal, *supra* note 9, at 192 (discussing the need for periodic risk assessments).

90. *See* Paul E. McGreal, *Best Practices in Corporate Compliance: Survey Results and Analysis—Part II*, 14 Fed. Ethics Rep. (CCH) (July 2007).

91. There may be good reason for an organization to have more than one code of conduct. *See* Joe Murphy & Win Swenson, *20 Questions to Ask About Your Code of Con-*

5. *Written compliance and ethics standards and procedures*: The organization's written standards and procedures are the operating documents of the compliance and ethics program. For example, every organization should have a sexual harassment policy that sets forth the organization's commitment to a harassment-free workplace, identifies what behavior the organization prohibits, lists the punishment for a violation of the policy, sets forth the procedures for asking questions and reporting violations, and establishes the procedures for investigating complaints and imposing discipline. The organization should adopt similar standards and procedures for its other major risks areas.[92] The standards and procedures should be periodically revised to take account of changes in the law and the organization's business environment.

6. *Employee and agent training*: For the compliance and ethics program to work, an organization must ensure that its employees and agents[93] understand and follow the policies and procedures. Simply distributing documents will not suffice. While documents memorialize the program and serve as references, they cannot substitute for training. The main training options are live presentations, videos, and computer-based modules, with the main tradeoff between cost and effectiveness. Testing comprehension is also important: An organization devoting valuable time and money to training will want to know whether the training is working.

7. *Lines of communication*: There are two main lines of communication in a compliance and ethics program: information and misconduct. First, the organization should open lines of communication to disseminate information about the compliance program. This includes helplines for seeking guidance about the compliance and ethics standards and procedures, as well as reporting lines that generate periodic, formal feedback about the operation of the compliance and ethics program.[94] Second, the organization should establish a system for receiving reports of possible misconduct. A reporting system must address issues such as the degree of confidentiality promised, whether anonymous reporting is permitted, and how to avoid conflicts of interest.[95]

---

duct, ETHIKOS & CORP. CONDUCT Q. (July-Aug. 2003), *available at* http://www.singerpubs.com/ethikos/html/20questions.html.

92. The major risk areas should have been identified and prioritized during the risk assessment. *See supra* note 89 and accompanying text.

93. The question of when and to what extent to include independent contractors in the compliance and ethics program is tricky. On the one hand, the organization does not want to exercise sufficient control over independent contractors to convert them into employees. On the other hand, the organization does not want to be seen as dealing with parties who do not follow similar corporate values.

94. For example, each business unit may have a compliance and ethics officer who makes quarterly reports to the chief compliance officer.

95. For example, a policy should not require that all reports of sexual harassment be made to a department supervisor, as a supervisor could be a harasser.

8. *Auditing and monitoring*: In addition to receiving reports, an effective compliance and ethics program should audit and monitor critical tasks for red flags. Such reviews can detect suspicious activity before it matures into a legal violation, or stop legal violations before they increase in scope or magnitude. For example, consider an organization concerned that its agents might bribe foreign government officials to obtain or retain business. The organization should have strict policies about payments and reimbursements to such agents, and should monitor and audit an agent's reimbursement requests for suspicious items.

9. *Enforcement, discipline, and positive incentives*: When a suspected violation is detected through reporting, monitoring, or auditing, the next step is to investigate and decide whether fire lies behind the smoke. The investigation must balance several interests: preventing retaliation against the person who discovered the potential violation, protecting the privacy of the accused, and avoiding obstruction of the investigation and additional possible legal violations. Once the investigation is completed, the organization must mete out appropriate discipline. Throughout the disciplinary process, the organization should document each step so it can prove that the investigation was thorough and fair.

In addition to discipline, recent compliance guidance suggests offering positive incentives to those who contribute to the compliance and ethics program.[96] For example, the organization can add compliance and ethics criteria to employee evaluations, or it could recognize employees who take steps to improve the operation or design of the compliance and ethics program. In doing so, however, the organization must avoid the perception that "compliance and ethics" is a pretext for rewarding favored employees.

10. *Periodic evaluation and improvement*: The compliance and ethics program must be a continuous feedback loop—compliance personnel must learn from their experiences. For example, training sessions or calls to the helpline may raise questions or concerns that expose a weakness in the program. Or monitoring, auditing, and reporting might identify risks or red flags that were not caught in the risk assessment. The compliance and ethics program must have a formal process for self-evaluation and modification to generate and take account of such feedback. In addition, to avoid conflicts of interest, some periodic evaluations should be conducted by personnel independent of those in charge of the compliance and ethics program.[97] For example, the organization could retain an outside expert to conduct the assessment, or

96. *See* U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(6) (2006), *available at* http://www.ussc.gov/2006guid/8b2_1.html.

97. *See, e.g.*, 31 C.F.R. § 103.125(d)(4) (2006) (anti-money laundering compliance program for a money services business should "[p]rovide for independent review to monitor and maintain an adequate program").

> designate personnel with relevant expertise from another unit, such as internal audit, to do so.[98]

In addition to the preceding ten steps, the government expects an organization to foster an institutional culture that supports the compliance and ethics program. A speech by Stephen Cutler, then-Director of the Securities and Exchange Commission's Division of Enforcement, put it this way: "[D]on't fall victim to a checklist mentality. . . . '[G]ood governance is not achieved by simply adhering to "checklists" of recommended "best practices.'"[99] Culture amounts to walking the compliance and ethics talk:

> All the words in the world mean nothing without deeds to support them. You have to pay more than lip service to values. You have to live them. The last few years have provided any number of examples of companies that failed to practice what they appeared to preach. Enron had the corporate slogan of "Respect, Integrity, Community, Excellence." To the employees and shareholders who lost their pensions or their life savings in the fraud, the words of that slogan ring rather hollow. In October 2003, at a conference of corporate directors, then Chairman and CEO of Computer Associates Sanjay Kumar bragged about his company's state-of-the-art corporate governance and business ethics practices. At the same time, according to the cases filed against him, Mr. Kumar was engaged in a large-scale fraud. As former IBM CEO Lou Gerstner has said, "you can't simply give a couple of speeches or write a new credo for the company and declare that a new culture has taken hold. You can't mandate it, can't engineer it. What you can do is create the conditions for transformation. You can provide incentives."[100]

Even if all ten of the above compliance and ethics tasks are performed to the state-of-the-art, the program is doomed if employees and agents doubt the organization's sincerity. And sincerity goes back to the old childhood adage that actions speak louder than words. Cutler concluded his speech with a series of practical examples: "managers themselves have to comply with the letter and the spirit of the rules";[101] "make integrity,

---

98. *See, e.g.*, DEP'T OF THE TREASURY: FINANCIAL CRIMES ENFORCEMENT NETWORK, FIN-2006-G012, FREQUENTLY ASKED QUESTIONS: CONDUCTING INDEPENDENT REVIEWS OF MONEY SERVICES BUSINESS ANTI-MONEY LAUNDERING PROGRAMS 2 (2006), *available at* http://www.fincen.gov/Guidance_MSB_Independent_Audits9-21.pdf ("Our regulations require an independent review, not a formal audit by a certified public accountant or third-party consultant. Accordingly, a money services business does not necessarily need to hire an outside auditor or consultant. The review may be conducted by an officer, employee or group of employees, so long as the reviewer is not the designated compliance officer and does not report directly to the compliance officer.").

99. Stephen M. Cutler, Dir., Div. of Enforcement, U.S. Sec. & Exch. Comm'n, Second Annual General Counsel Roundtable: Tone at the Top: Getting it Right (Dec. 3, 2004), *available at* http://www.sec.gov/news/speech/spch120304smc.htm (quoting RICHARD C. BREEDEN, RESTORING TRUST: REPORT TO THE HON. JED S. RAKOFF, THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK, ON CORPORATE GOVERNANCE FOR THE FUTURE OF MCI, INC. 30 (Aug. 2003), *available at* http://news.findlaw.com/hdocs/docs/worldcom/corpgov82603rpt.pdf).

100. *Id.*

101. *Id.*

ethics and compliance part of the promotion, compensation and evaluation processes";[102] and "make it clear that you won't tolerate compliance risks—even if that means losing a lucrative piece of business or a client or a transaction."[103] To return to a metaphor from the beginning of this section, if the risk assessment is the compliance and ethics program's blue print, then the organization's culture is the foundation.

B. COMPLIANCE AND THE CONSTITUTION: *WHALEN V. ROE*

The Supreme Court's decision in *Whalen v. Roe*[104] illustrates how an ethics and compliance program (though the Court never called it that) can influence constitutional analysis. There, a New York law targeted the problem posed by diversion of drugs with legal uses "into unlawful channels."[105] For example, patients and physicians might use multiple or fake prescriptions to circumvent the state's drug control laws. To combat such abuse, one provision of the law prescribed record-keeping requirements for certain drugs:

> [A]ll prescriptions for [the specified] drugs [must] be prepared by the physician in triplicate on an official form. The completed form identifies the prescribing physician; the dispensing pharmacy; the drug and dosage; and the name, address, and age of the patient. One copy of the form is retained by the physician, the second by the pharmacist, and the third is forwarded to the New York State Department of Health in Albany. A prescription made on an official form may not exceed a 30-day supply, and may not be refilled.[106]

The database was supposed to reduce drug misuse in two ways. First, the state could analyze the data for patterns that indicated illegal use.[107] Second, enhanced detection would deter misuse.[108]

Similar to the data mining described above, the New York database accumulated immense amounts of data concerning legitimate activity (here, legal drug prescriptions) to detect the few cases of illegal activity (here, drug abuse). For example, during the first twenty months that the

---

102. *Id.*
103. *Id.*
104. 429 U.S. 589 (1977).
105. *Id.* at 591.
106. *Id.* at 593.
107. The special commission that proposed the database described this process as follows:

> Once the department has received the copies, it will be able to compile data which will uncover irregularities such as forgeries, fraudulent obtaining of schedule[d] substances, and thefts of prescription blanks and their misuse by unauthorized persons. The information received by the department will show if a patient has obtained prescriptions by going from doctor to doctor, or if stolen prescriptions are being used. This procedure will also indicate where there has been an over-prescribing or over-dispensing of [specified] drugs.

Brief of Appellant at 6, *Whalen v. Roe*, 429 U.S. 589 (1977) (No. 75-839), 1976 WL 1814-00. Of course, this method is not perfect, as it would not detect a person who obtains multiple prescriptions under different names.
108. *Whalen*, 429 U.S. at 598.

database operated, the state collected an average of 100,000 prescription forms per month, and the data contributed to only two drug misuse investigations.[109] This led the appellees to characterize the database as "a vast state system which uses a dragnet more likely to expose the names of patients seeking drugs for legitimate medically indicated use than those obtaining drugs for illicit purposes."[110]

The plaintiffs, who were prescribed drugs covered by the record-keeping provision, argued that the database threatened harm due to misuse or disclosure of their data. Misuse could consist of the state stereotyping an individual in the database as a drug addict and discriminating against the person on that basis. Disclosure could occur either through a state employee leaking the information or an outsider gaining unauthorized access.[111] These fears, in turn, allegedly discouraged patients from seeking needed medications.[112] Note that these arguments parallel those regarding modern domestic surveillance: Centralized collection of data exponentially increases the harm posed by abuse of the data.[113]

The Supreme Court upheld the database, largely due to state-mandated controls that minimized the threat of abuse:[114]

---

109. *Id.* at 593–95. In its amicus brief, the State of California stated that it had used its comparable database in over three hundred investigations in the preceding two years. *See* Brief for State of California as Amicus Curaie Supporting Appellants at note 2, *Whalen v. Roe*, 429 U.S. 589 (1977) (No. 75-839), 1975 WL 173716.

110. Brief of Appellees at 17, *Whalen v. Roe*, 429 U.S. 589 (1977) (No. 75-839), 1976 WL 181402. The appellees also challenged the efficacy of the database. For example, while a search of the records would identify a person who obtained multiple prescriptions under the same name, it could not detect a person who used an alias to obtain the prescriptions. *Id.*

111. *Whalen*, 429 U.S. at 600–01 ("Health Department employees may violate [state law] by failing, either deliberately or negligently, to maintain proper security.").

112. Brief of Appellees at 9, *Whalen v. Roe*, 429 U.S. 589 (1977) (No. 75-839), 1976 WL 18401.

113. *See supra* notes 16–17 and accompanying text; POSNER, SUICIDE PACT, *supra* note 59, at 135 ("[U]ntil recently the information that people voluntarily disclosed to vendors, licensing bureaus, hospitals, and so on was scattered, fugitive (because the bulkiness of paper records usually causes them to be discarded as soon as they lose their value to the enterprise), and searchable only with great difficulty—which provided further incentive to discard information. So although one had voluntarily disclosed private information on innumerable occasions to sundry recipients, one retained as a practical matter a great deal of privacy.").

114. The appellees attacked the state's efforts to prevent misuse or disclosure of the data:

> [T]he plaintiffs presented uncontradicted testimony of a computer expert that personnel checks were inadequate, the turnover in temporary help was dangerous, the physical security of the building nonexistent, and the data security system unsophisticated.
>
> The state's only response to the plaintiffs' evidence about the system's lack of security was to introduce the deposition testimony of . . . the director of the Bureau of Controlled Substances Licensing. [The director] admitted that there were no written procedures for processing printouts from the system, that he was unaware of the nature of employment background checks, if any, which were conducted on personnel employed by the data center, that he did not know whether or not any personnel had criminal records, that of the 17 employees in the State Bureau "We may have five or six, possibly seven new ones," within the past year, and that he did not know the background of

> [P]rescription forms are delivered to a receiving room at the Department of Health in Albany each month. They are sorted, coded, and logged and then taken to another room where the data on the forms is recorded on magnetic tapes for processing by a computer. Thereafter, the forms are returned to the receiving room to be retained in a vault for a five-year period and then destroyed as required by the statute. The receiving room is surrounded by a locked wire fence and protected by an alarm system. The computer tapes containing the prescription data are kept in a locked cabinet. When the tapes are used, the computer is run "off-line," which means that no terminal outside of the computer room can read or record any information. Public disclosure of the identity of patients is expressly prohibited by the statute and by a Department of Health regulation. Willful violation of these prohibitions is a crime punishable by up to one year in prison and a $2,000 fine.[115]

Here, one can glimpse aspects of an effective compliance and ethics program. For example, the state had a policy prohibiting the disclosure of patient information as well as specified punishment for a violation. Further, the Court saw evidence that the controls actually worked, as there was no evidence of problems with the New York database or similar databases in two other states.[116] One would want to know, however,

---

> temporary employees, the employment testing or processing for selecting them, or whether they had criminal records or not.

Brief of Appellees at 11–12, *Whalen v. Roe*, 429 U.S. 589 (1977) (No. 75-839), 1976 WL 181402. Note that these assertions raise several concerns about whether the state managed the database under an effective compliance and ethics program. For example, the state allegedly took insufficient steps to ensure that those who handled the data were trustworthy. This goes against the Sentencing Guidelines requirement that an effective compliance and ethics program use "due diligence" in performing background checks on employees who will exercise "substantial authority" within the organization. U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(3) (2006), *available at* http://www.ussc.gov/2006guid/862_/.html ("the organization shall use reasonable efforts not to include within the substantial authority personnel of the organization any individual whom the organization knew, or should have known through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program"). Further, the state allegedly had no written procedures regarding the handling of the data, and so presumably never trained its personnel on how to handle the data. As discussed below, the federal government now imposes such requirements on private firms that handle private customer data. *See infra* Part IV.C. The lower court, however, made no findings on the adequacy of the state's data security controls because it concluded that the database as a whole lacked a sufficient law enforcement basis. *See* Roe v. Ingraham, 403 F. Supp. 931, 933, 938 (S.D.N.Y. 1975), *overruled sub nom.*, *Whalen v. Roe*, 429 U.S. 589 (1977) (No. 75-839), 1976 WL 181402; Brief of Appellees at 11, *Whalen v. Roe*, 429 U.S. 589 (1977) ("The Court did not reach the question of the security of the state's computer system").

115. *Whalen*, 429 U.S. at 593–95.

116. *Id.* at 590 ("There is no support in the record or in the experience of the two States that New York program emulates, for assuming that the statute's security provisions will be improperly administered."). Interestingly, the Foreign Intelligence Surveillance Court has found that federal officials had submitted 75 warrant affidavits that contained "misstatements and omissions of material facts," and that executive branch officials had improperly shared foreign intelligence information with domestic law enforcement officials. *In re* All Matters Submitted to For. Intel. Surv. Ct., 218 F. Supp. 2d 611, 620–21 (For. Intel. Surv. Ct.), *rev'd on other grounds*, *In re* Sealed Case, 310 F.3d 717 (For. Intel. Surv. Rev. 2002). Judge Richard Posner has proposed a strict separation of foreign intelligence and domestic

whether the state had other compliance functions, such as whether there was auditing or monitoring for violations of this non-disclosure rule.

The Court concluded its opinion by leaving open the question of what role the existence of data security measures should play in future analysis:

> A final word about issues we have not decided. We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. Recognizing that in some circumstances that duty arguably has its roots in the Constitution, nevertheless New York's statutory scheme, and its implementing administrative procedures, evidence a proper concern with, and protection of, the individual's interest in privacy. We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data whether intentional or unintentional *or by a system that did not contain comparable security provisions*. We simply hold that this record does not establish an invasion of any right or liberty protected by the Fourteenth Amendment.[117]

This passage yields two points relevant to the current analysis. First, in reviewing the constitutionality of government collection, analysis, and storage of citizen data, a court should consider what safeguards the government has implemented to prevent improper use or disclosure of the data. These safeguards are in essence compliance and ethics measures tailored to data security. Second, since *Whalen* was decided in 1977, the understanding and requirements of an effective compliance and ethics program in general, and for data security specifically, have changed dramatically. Indeed, as the next section explains, recent federal regulations prescribe rather detailed compliance measures for firms that handle customer data. In Part V, this Essay suggests that *Whalen*'s insight about the constitutional relevance of compliance measures be updated to take account of the increased formality and sophistication of modern compliance and ethics programs.

---

law enforcement, with significant criminal penalties to deter violations. POSNER, SUICIDE PACT, *supra* note 59, at 151–52.

117. *Whalen*, 429 U.S. at 605–06 (emphasis added); *see also id.* at 607 ("In this case, as the Court's opinion makes clear, the State's carefully designed program includes numerous safeguards intended to forestall the danger of indiscriminate disclosure. Given this serious and, so far as the record shows, successful effort to prevent abuse and limit access to the personal information at issue, I cannot say that the statute's provisions for computer storage, on their face, amount to a deprivation of constitutionally protected privacy interests, any more than the more traditional reporting provisions.") (Brennan, J., concurring).

C. Modern Compliance Requirements for Data Privacy

This Part discusses two areas where federal law requires private firms to design and implement compliance and ethics measures to protect customer data: First, the Federal Trade Commission's enforcement actions regarding customer data collected through a company's web site; second, federal banking regulations that require protection of customer data. As the following discussion illustrates, the federal government requires heightened diligence of private firms that handle customer data.

The Federal Trade Commission Act charges the Federal Trade Commission ("FTC") with enforcing the Act's prohibition of "unfair or deceptive acts or practices in or affecting commerce."[118] The FTC has recently applied this provision to privacy promises made by commercial websites.[119] The typical privacy policy makes specific assurances about the protection and use of customer information, such as name, address, phone number, and credit card information. The FTC has argued that these assurances impliedly assert that the vendor takes adequate measures to protect customer data. If the vendor does not in fact have such measures in place, the implied assertion (and thus the privacy policy) is false—a deceptive act in violation of the FTC Act.

To illustrate this type of violation, consider the FTC's enforcement action against Petco Animal Supplies, Inc.[120] The FTC alleged that purchasers on Petco's website had to submit "personal information, including, but not limited to, name, address, and credit card number and expiration date."[121] The information was then stored "in a database that supports or connects to [Petco's] website."[122] Petco's website made the following assurance about the handling of customer information: "The server encrypts all of your information; no one except you can access it."[123] Yet, the FTC alleged, Petco did not store customer data in en-

118. 15 U.S.C. §§ 45(a)(1)–(2) (2005).

119. In 1999, the FTC issued its first complaint based on this theory against the web-hosting service GeoCities. Complaint, *In re* GeoCities, 127 F.T.C. 94 (F.T.C. 1999) (No. C-3850), *available at* http://www.ftc.gov/os/1999/02/9823015cmp.htm.

120. Complaint, *In re* Petco Animal Supplies, Inc., No. 032-3221, 2004 WL 2682593 (F.T.C. Nov. 8, 2004), *available at* http://www.ftc.gov/os/caselist/0323221/041108comp0323221.pdf [hereinafter Petco Complaint]. For a collection of FTC enforcement actions regarding website privacy promises, see Federal Trade Commission: Privacy Initiatives: Unfair & Deceptive Practices: Enforcement, http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html (last visited Aug. 4, 2007).

121. Petco Complaint, *supra* note 120, at 1.

122. *Id.*

123. *Id.* at 2; *see also* Complaint at 2, *In re* Microsoft Corp., No. C-4069, 2002 WL 31881313 (F.T.C. Dec. 20, 2002), *available at* http://www.ftc.gov/os/caselist/0123240/microsoftcmp.pdf ("[Microsoft] did not maintain a high level of online security by employing sufficient measures reasonable and appropriate under the circumstances to maintain and protect the privacy and confidentiality of personal information obtained from or about consumers in connection with the Passport and Passport Wallet services. In particular, respondent failed to implement and document procedures that were reasonable and appropriate to: (1) prevent possible unauthorized access to the Passport system; (2) detect possible unauthorized access to the Passport system; (3) monitor the Passport system for potential vulnerabilities; and (4) record and retain system information sufficient to perform security audits and investigations.").

crypted form, and the stored data was "vulnerable to commonly known or reasonably foreseeable attacks from third parties."[124] Indeed, the FTC issued its complaint after a Petco website user allegedly gained unauthorized access to customer information.[125]

In settling the case, the FTC's Decision and Order directed Petco to design and implement an effective compliance and ethics program covering protection of customer information.[126] The relevant provision of the Decision and Order is worth quoting in full, as it indicates what data protection measures the government itself believes are effective. The quoted text is annotated by footnotes that identify the ten compliance and ethics measures discussed above:[127]

> IT IS FURTHER ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the online advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers.[128] Such program, the content and implementation of which must be fully documented in writing,[129] shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's

---

124. Petco Complaint, *supra* note 120, at 3. ("In truth and in fact, the personal information respondent obtained from consumers through www.PETCO.com was not maintained in an encrypted format and was accessible to persons other than the consumer providing the information."). *See also* Complaint at 2, *In re* Guidance Software, Inc., No. C-4187, 2007 WL 183340 (F.T.C. Mar. 30, 2006), *available at* http://www.ftc.gov/os/caselist/0623057/0623057%20-Guidance%20complaint.pdf (alleging the following lapses: "[R]espondent: (1) stored the information in clear readable text; (2) did not adequately assess the vulnerability of its web application and network to certain commonly known or reasonably foreseeable attacks, such as "Structured Query Language" (or "SQL") injection attacks; (3) did not implement simple, low-cost, and readily available defenses to such attacks; (4) stored in clear readable text network user credentials that facilitate access to sensitive personal information on the network; (5) did not use readily available security measures to monitor and control connections from the network to the internet; and (6) failed to employ sufficient measures to detect unauthorized access to sensitive personal information.")

125. Petco Complaint, *supra* note 120, at 3–4.

126. Decision and Order, *In re* Petco Animal Supplies, Inc., No. C-4133, 2005 WL 681260 (F.T.C. Mar. 4, 2005), *available at* http://www.ftc.gov/os/caselist/0323221/050308do023221.pdf.

127. *See supra* notes 88–98 and accompanying text.

128. This opening sentence implicates involvement of the organization's governing authority. *See supra* text at pg. 1586. Presumably, the board has been periodically briefed on the FTC's enforcement and approved the ultimate resolution. Board oversight of the company's compliance with the Decision and Order would fall within the board's overall responsibility to oversee the company's reporting and compliance systems. *See supra* note 88 and discussion on pp. 1585–89. *See also In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959 (Del. Ch. 1996). The board's oversight should include periodic reporting on the required compliance and ethics program as well as ensuring that adequate resources are committed to design and implementation of the program.

129. This provision implicitly requires the written documents entailed by a compliance and ethics program, such as a code of conduct provision and company policies regarding data security. *See supra* note 91–92 and accompanying text.

activities, and the sensitivity of the personal information collected from or about consumers,[130] including:

A. the designation of an employee or employees to coordinate and be accountable for the information security program.[131]

B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks.[132] At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management;[133] (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response[134] to attacks, intrusions, or other systems failures.

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment,[135] and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.[136]

D. the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by subparagraph C,[137] any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.[138]

In short, the FTC's Decision and Order requires all the elements of an effective compliance and ethics program.

---

130. This sentence implicitly requires a risk assessment. *See supra* note 89 and accompanying text. The program cannot be "appropriate to respondent's size and complexity, the nature and scope of respondent's activities," unless the company assesses the risks posed by these aspects of its business.

131. This provision explicitly requires designation of compliance personnel. *See supra* note 90 and accompanying text.

132. Here, the FTC specifically requires a risk assessment. *See supra* note 89 and accompanying text.

133. This is an explicit requirement of employee training. *See supra* note 93 and accompanying text.

134. Response to security breaches would presumably include investigation and (when appropriate) discipline for violations of any internal policies or procedures. *See supra* note 96 and accompanying text.

135. Here again the Decision and Order requires written policies and procedures. *See supra* note 92 and accompanying text.

136. This is an explicit requirement of monitoring and auditing. *See supra* discussion on pg. 1588.

137. This is an explicit requirement that the company periodically evaluate and improve its compliance and ethics program. *See supra* notes 97–98 and accompanying text.

138. Decision and Order at 2–3, *In re* Petco Animal Supplies, Inc., No. C-4133, 2005 WL 681260 (F.T.C. MAR. 4, 2005) *available at* http://www.ftc.gov/os/caselist/0323221/050308do0323221.pdf. This provision is typical of other Consent Orders entered by the FTC. *See, e.g.*, Agreement Containing Consent Order at 3–4, *In re* Guidance Software, Inc., No. 062-3057, 2006 WL 3478138 (F.T.C. Nov. 16, 2006), *available at* http://www.ftc.gov/os/caselist/0623057/0623057%20-Guidance%20consent%20agreement.pdf.

By rule, FTC banking regulations similarly require financial institutions to implement compliance and ethics safeguards for customer information.[139] The rules are promulgated under the Gramm-Leach-Bliley Act,[140] which recognizes that "each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[141] The Act requires financial institutions to make certain disclosures regarding the privacy and use of customer information, and directs federal agencies to promulgate compliance standards for "financial institutions . . . subject to their jurisdiction."[142] In response to this directive, the FTC promulgated the Standards for Safeguarding Customer Information Rule ("Safeguards Rule"),[143] which has the purpose of "set[ting] forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information."[144] The Safeguards Rule requires specified financial institutions to "develop, implement, and maintain [an] information security program," and defines the elements of such a program in a similar manner to the website privacy cases just discussed. And, as with website privacy, the FTC has brought enforcement actions for failure to abide by the Safeguards Rule.[145]

---

139. The FTC also has a set of guiding principles for businesses that handle customer personal information:

> 1. Take stock. Know what personal information you have in your files and on your computers.
> 2. Scale down. Keep only what you need for your business.
> 3. Lock it. Protect the information that you keep.
> 4. Pitch it. Properly dispose of what you no longer need.
> 5. Plan ahead. Create a plan to respond to security incidents.

FEDERAL TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS 3, *available at* http://www.ftc.gov/bcp/edu/pubs/business/privacy/bus69.pdf (last visited Oct. 23, 2007).

140. 15 U.S.C. §§ 6801–6809 (2002).

141. *Id.* § 6801(a); *see also id.* § 6804(a)(1) (granting authority to "[t]he Federal banking agencies, the National Credit Union Administration, the Secretary of the Treasury, the Securities and Exchange Commission, and the Federal Trade Commission to draft regulations to enforce the Act").

142. *Id.* § 6805(a)(7) (provision regarding the FTC).

143. 16 C.F.R. §§ 314.1–314.5 (2007). The FTC has also promulgated the Privacy of Consumer Financial Information Rule, 16 C.F.R. §§ 313.1–313.3 (2007), which implements the Act's disclosure requirements. All agencies covered by the Gramm-Leach-Bliley Act have recently joined in proposing a model privacy form to be used by covered institutions. *See* Interagency Proposal for Model Privacy Form Under the Gramm-Leach-Bliley Act, 72 Fed. Reg. 14,940 (Mar. 29, 2007).

144. 16 C.F.R. § 314.1(a) (2007). *See* Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 30, app. B (2007).

145. *See, e.g.*, Complaint at 1, *In re* Sunbelt Lending Servs., Inc., No. C-4129, 2005 WL 120875 (F.T.C. Jan. 30, 2005) *available at* http://www.ftc.gov/os/caselist/0423153/050107comp0423153.pdf. There, the FTC alleged:

> [R]espondent failed to assess the risks to its customer information; implement reasonable policies and procedures in key areas, such as employee training and appropriate oversight of the security practices of loan officers working from remote locations; or oversee the collection and handling of information through the Sunbelt Web site. Respondent also failed to take

Separate from the FTC's Safeguards Rule, the Federal Financial Institutions Examination Council, representing five federal agencies,[146] has promulgated a joint rule prescribing information security program standards for the financial institutions within their jurisdiction.[147] As do the FTC standards, the Council's standards incorporate the ten compliance and ethics program measures discussed above, including:

- A bank's board of directors shall "[a]pprove" and "[o]versee the development, implementation, and maintenance of the bank's information security program, including assigning specific responsibility for its implementation and reviewing reports from management."[148]
- A bank shall "report to its board or an appropriate committee of the board at least annually" regarding the operation of the information security program.[149]
- A bank shall both assess the risk and likelihood of "unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems" and "the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks."[150]
- A bank shall implement controls designed to protect customer information from unauthorized access.[151]
- A bank shall "[t]rain staff to implement the bank's information security program."[152]
- A bank shall "[r]egularly test the key controls, systems and procedures of the information security program. . . . . Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs."[153]
- A bank shall monitor and audit for security breaches, and implement procedures for responding to breaches.[154]

---

steps to ensure that its service providers were providing appropriate security for Sunbelt's customer information.

Id. at 2. The Decision and Order in the case required Sunbelt to implement the required information security program and to report the results of periodic program evaluations to the FTC. Decision and Order at 3, *In re* Sunbelt Lending Servs., Inc., No. C-4129, 2005 WL 120875 (F.T.C. Jan. 30, 2005) *available at* http://www.ftc.gov/os/caselist/0423153/050107do0423153.pdf.

146. The five agencies are the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision. *See* Federal Financial Institutions Examination Council Home Page, http://www.ffiec.gov/ (last visited Aug. 4, 2007). In addition, the Council includes the State Liaison Committee. *Id.*

147. Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 208, app. D-2 (2007).

148. 12 C.F.R. pt. 208, app. D-2 ¶ III.A.

149. 12 C.F.R. pt. 208, app. D-2 ¶ III.F.

150. 12 C.F.R. pt. 208, app. D-2 ¶ III.B.

151. 12 C.F.R. pt. 208, app. D-2 ¶ III.C.1.

152. 12 C.F.R. pt. 208, app. D-1 ¶ C.2.

153. 12 C.F.R. pt. 208, app. D-2 ¶ III.C.3.

154. 12 C.F.R. pt. 208, app. D-1 ¶¶ III.C.1.f. & g.

- A bank shall conduct "[b]ackground checks for employees who are authorized to access to customer information . . . ."[155]

The standards discussed in this Part show how the federal government requires private firms to design and implement compliance and ethics programs that protect the privacy of customer personal information.[156] In designing and operating these programs, private business has evolved substantial consensus regarding the minimum criteria for an effective compliance and ethics program. As discussed in the next Part, these criteria provide federal judges with standards to guide separation of powers analysis.

V. PUTTING IT ALL TOGETHER: A SEPARATION OF POWERS PROPOSAL

The preceding parts of this Essay discuss aspects of the separation of powers, constitutional protections for private information, and compliance and ethic programs. The following discussion assimilates the preceding observations into four propositions, and then offers a proposed tweak to our separation of powers analysis.

First, separation of powers requires some form of checks and balances among the three branches of the federal government. The checks and balances must be robust enough to prevent the accumulation of federal power in a single branch of government, even if that accumulation is in a narrow area. The need for checks and balances derives from human nature—those entrusted with government power will seek to expand their power.

Second, when the subject is individual liberty, it is important that the federal judiciary play a meaningful role in checking the power of the other two branches. This is because the popularly accountable branches—the President and Congress—may not be adequately motivated to protect individual liberties, as when the claimed liberty is unpopular.

Third, modern domestic surveillance, even in aid of foreign intelligence, entails the collection and storage of massive amounts of private data concerning United States citizens. Citizens rightly fear that such data could be either misused or improperly disclosed, raising issues of individual liberty that (at times) may be unpopular. Separation of powers suggests that the federal judiciary ought to be involved in checking Congress and the President in this area. And *Whalen v. Roe*[157] further suggests that one such check ought to be judicial review to determine

155. 12 C.F.R. pt. 208, app. D-2, supp. A ¶ II.

156. *See also* Health Insurance Portability and Accountability Act, Pub. L. 104–191, 110 Stat. 1936 (1996); CHRISTOPHER WOLF, PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE § 5 (2006); Vincent Serpico, Denise Landers & Damon A. Terrill, *Making Sense of U.S. State Data Privacy Law*, 119 BANKING L.J. 462, 462 (2002).

157. 429 U.S. 589 (1977).

whether the President and Congress have implemented adequate safeguards to prevent misuse or improper disclosure of private information.

Fourth, what is today called a corporate compliance and ethics program can provide needed safeguards against misuse or improper disclosure of private data. Since the Court decided *Whalen v. Roe*[158] in 1977, the federal government, the states, and private industry have developed both general criteria for effective compliance and ethics programs, and specific criteria for data security programs. These criteria are specific enough for regulators,[159] courts,[160] and prosecutors[161] to apply in determining whether a regulated entity has taken adequate compliance measures. Thus, the separation of powers doctrine should incorporate the modern compliance and ethics program standards discussed in Part IV. Specifically, courts should ask whether the President and Congress have established controls to prevent misuse or improper disclosure of private information of United States citizens collected and stored during domestic foreign intelligence surveillance.

A common objection to greater judicial review of federal antiterrorism measures and defense of greater judicial deference to the President and Congress is the courts' comparative lack of expertise in the area.[162] As Judge Posner has put it, "[j]udges aren't *supposed* to know much about national security."[163] Eric Posner and Adrian Vermeule have also stated that the "novelty of the threats and of the necessary responses makes judicial routines and evolved legal rules seem inapposite, even obstructive."[164]

One need not dispute these claims to endorse this Essay's proposal.[165] First, as discussed above, strong consensus exists among regulators and private firms about the essential components of an effective compliance and ethics program. Of course, there is discussion and debate regarding some details, such as whether the corporate compliance officer ought to report through the organization's legal department or directly to the CEO or a board committee. But courts can apply the consensus standards and give deference where consensus runs out.

Second, we know that evaluating compliance and ethics programs is not beyond judicial competence because courts already do so in several contexts. As discussed above, the United States Sentencing Guidelines

158. *Id.*

159. *See supra* notes 98–103 and accompanying text.

160. *See* U.S. SENTENCING GUIDELINES MANUAL § 8B2.1 (2006), *available at* http://www.ussc.gov/2006guid/8b2_1.html.

161. *See* Memorandum from Paul J. McNulty, Deputy Attorney Gen., to Heads of Dep't Components and U.S. Attorneys 12-15 (Dec. 12, 2006), *available at* http://www.corporatecompliance.com/events/07docs/AC_McNulty/FTL1-20075/v/Paul%201.pdf.

162. ERIC A. POSNER & ADRIAN VERMEULE, TERROR IN THE BALANCE: SECURITY, LIBERTY, AND THE COURTS 31 (2007) ("Judges are generalists, and the political insulation that protects them from current politics also deprives them of information, especially information about novel security threats and necessary responses to those threats.").

163. POSNER, SUICIDE PACT, *supra* note 59, at 37 (emphasis in original).

164. POSNER & VERMEULE, *supra* note 162, at 18.

165. For a criticism of these calls for judicial deference, see Solove, *supra* note 64, at 2.

direct federal courts to assess the effectiveness of a corporate defendant's compliance and ethics program as a mitigating factor in criminal sentencing.[166] In federal sexual harassment and civil rights cases, federal courts assess a corporate defendant's compliance and ethics program in litigating a defense to vicarious liability.[167] Under state corporate law, recent decisions from the Delaware Supreme Court suggest that that state's courts will now assess whether a corporate board has adhered to compliance best practices in ruling on a motion to dismiss claims against directors.[168] And courts and agencies are increasingly incorporating compliance and ethics efforts into legal tests.[169] It is far too late in the day to claim that evaluating compliance and ethics programs is beyond judicial competence.

The remaining question is whether corporate compliance and ethics measures ought to be a safe harbor or a constitutional requirement. Here, Justice Jackson's admonition looms large: "While the Constitution diffuses power the better to secure liberty, it also contemplates that practice will integrate the dispersed powers into a workable government."[170] This counsels a safe harbor approach for three reasons. First, while corporate compliance and ethics programs have proven effective at checking private misconduct, they may not be the only (or even best) measure for checking abuse of government power. Consequently, this Essay's modest proposal ought to proceed modestly, recognizing the inherent limits of human knowledge.[171]

Second, even a safe harbor provides the powerful incentive of a specific outcome—here, constitutionality—whereas alternative measures offer uncertainty. Further, this safe harbor holds the benefit of identifiable criteria that provide concrete guidance for government action. In designing and implementing a compliance and ethics program to protect citizen

166. *See supra* notes 90, 87, 95, 111 and accompanying text.

167. *See* Kolstad v. Am. Dental Ass'n, 527 U.S. 526, 545–46 (1999) (good faith compliance efforts can be a defense to punitive damages liability in federal civil rights action); Faragher v. City of Boca Raton, 524 U.S. 775, 807 (1998); Burlington Indus., Inc. v. Ellerth, 524 U.S. 742, 765 (1998) (reasonable efforts to detect and remedy incidents of sexual harassment can be defense to employer liability) (same).

168. *See* Stone v. Ritter, 911 A.2d 362, 372–73 (Del. 2006); Desimone v. Barrows, 924 A.2d 908 (Del. Ch. 2007); *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 969 (Del. Ch. 1996); *see also* Paul E. McGreal, *Corporate Compliance Survey*, 62 BUS. LAW. (forthcoming 2007) (discussing the relevance of best practices to claim that directors violated their duty to not consciously disregard oversight of the corporation's compliance and ethics program).

169. *See* W.G. Yates & Sons Constr. Co. v. Occupational Safety & Health Review Comm'n, 459 F.3d 604, 608–09 (5th Cir. 2006); Commodity Futures Trading Comm'n v. Carnegie Trading Group, Ltd., 450 F. Supp. 2d 788, 803–04 (N.D. Ohio 2006); U.S. v. Merck-Medco Managed Care, L.L.C., 336 F. Supp. 2d 430, 440–41 (E.D. Pa. 2004) (in a lawsuit under the Federal False Claims Act, the lack of an effective corporate compliance and ethics program is probative evidence of whether the corporate defendant recklessly disregarded the risk that it was submitting false claims to the government).

170. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 635 (1952) (Jackson, J., concurring in the judgment).

171. *See generally* FRIEDRICH A. HAYEK, THE FATAL CONCEIT: THE ERRORS OF SOCIALISM (W.W. Bartley III ed., 1988).

data, the federal government can benchmark against private entities that must perform the same tasks for private customer data.[172] Indeed, in some instances the federal government will be analyzing data obtained from private databases that are themselves legally required to have data security compliance and ethics programs.[173]

Third, judges will be more timid in identifying and applying compliance and ethics principles if doing so poses a constitutional bar to government action. As Judge Posner has written:

> Judges, knowing little about the needs of national security, are unlikely to oppose their own judgment to that of the executive branch, which is responsible for the defense of the nation. They are especially unlikely to interpose *constitutional* objections because of the difficulty of amending the Constitution to correct judicial error.[174]

The safe harbor frees judges to rule definitively on compliance and ethics principles, knowing that the federal government may experiment with alternate arrangements.

To summarize, this Essay proposes the following separation of powers analysis. When the federal government collects private information of United States citizens while conducting foreign intelligence surveillance, separation of powers demands that adequate checks and balances protect against abuse or misuse of the information. The government may carry this burden by demonstrating that its data collection, analysis, and storage operate under an effective compliance and ethics program. If the government does not carry this burden, it must then show that its surveillance includes internal controls with the same level of protection provided by an effective compliance and ethics program.

Though not discussed here, this separation of powers analysis logically extends to all government programs that handle private citizen data. For example, a report by the United States General Accounting Office ("GAO") notes that "52 [federal government] agencies are using or are planning to use data mining."[175] The Privacy Act[176] and the Federal Information Security Management Act of 2002[177] require that agencies take measures to protect their data from improper disclosure, and the Office of Management and Budget[178] and the National Institute of Standards

---

172. *See supra* Part IV.A. and accompanying text.

173. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-05-866, DATA MINING: AGENCIES HAVE TAKEN KEY STEPS TO PROTECT PRIVACY IN SELECTED EFFORTS, BUT SIGNIFICANT COMPLIANCE ISSUES REMAIN 2 (Aug. 2005), *available at* http://www.gao.gov/new.items/d05866.pdf [hereinafter GAO COMPLIANCE REPORT] (federal agency data-mining projects use data from "private sector sources (such as credit card companies)").

174. *See* POSNER, SUICIDE PACT, *supra* note 59, at 9.

175. *See* GAO DATA MINING REPORT, *supra* note 65, at 2.

176. *See* 5 U.S.C. §§ 522a(e)(9)–(10) (2005).

177. *See* 44 U.S.C. §§ 3541–3549 (2005).

178. *See, e.g.*, Memorandum from Jacob J. Lew to Heads of Executive Departments and Agencies Guidance on Inter-Agency Sharing of Personal Data-Protecting Personal Privacy (Dec. 20, 2000) *available at* http://www.whitehouse.gov/omb/memoranda/m01-05.html; Guidance on Privacy Act Implications of "Call Detail" Programs to Manage Employees' Use of the Government's Telecommunication System, 52 Fed. Reg. 12,290 (Apr. 20, 1987),

and Technology provide guidance on compliance.[179] The GAO, however, has found that some agencies have not met the statutory or regulatory standards for safeguarding their data.[180] Under this Essay's thesis, these failures would become relevant to separation of powers analysis.

CONCLUSION

Throughout American history, the Supreme Court has applied the Constitution to changed circumstances. After 9/11, the Court must do so again, as some battles in the war on terror threaten our constitutional commitment to liberty and privacy. While the Bill of Rights often takes center stage when individual liberty is threatened, we must not forget that separation of powers—our system of checks and balances—is the first line of defense against such incursions. Our timeless commitment to separated power must now be applied to the federal government's timely efforts to identify terrorists and prevent their attacks. This Essay proposes that separation of powers analysis look to the evolving discipline of corporate compliance and ethics for guidance. Over the last half century, businesses have accumulated vast expertise on checking and balancing the exercise of private authority to protect shareholder value. The federal government ought to employ similar measures to protect our constitutional values.

---

available at http://www.whitehouse.gov/omb/inforeg/guidance_privacy_act.pdf; Responsibilities for the Maintenance of Records About Individuals by Federal Agencies, 40 Fed. Reg. 28,948 (July 9, 1975). Several OMB Privacy Act guidance documents are collected on the OMB's webpage. *See* White House, Office of Management and Budget, Privacy Guidance, General, http://www.whitehouse.gov/omb/privacy/general.html (last visited Aug. 4, 2007).

179. NIST compliance guidance is collected on the agency's webpage. *See* NIST, Computer Security Division: Computer Security Resource Center, FISMA Implementation Project, Compliance, *available at* http://csrc.nist.gov/sec-cert/ca-compliance.html (last visited Aug. 4, 2007).

180. *See* GAO COMPLIANCE REPORT, *supra* note 173, at 14–15; *see also* U.S. GEN. ACCOUNTING OFFICE, GAO-03-304, PRIVACY ACT: OMB LEADERSHIP NEEDED TO IMPROVE AGENCY COMPLIANCE (June 2003), *available at* http://www.gao.gov/new.items/d03304.pdf; OFFICE OF MGMT. & BUDGET, FED. INFO. SEC. MGMT. ACT (FISMA) 2004 REP. TO CONG. 4-5 (Mar. 1, 2005), *available at* http://www.whitehouse.gov/omb/inforeg/2004_fisma_report.pdf (discussing the federal government's compliance with the FISMA data security requirements).