Duquesne Law Review

Volume 42 | Number 4 Article 3

2004

Civil Liberty and the Response to Terrorism

Paul Rosenzweig

Civil Liberty and the Response to Terrorism

Paul Rosenzweig[*]

> In any civilized society the most important task is achieving a proper balance between freedom and order. In wartime, reason and history both suggest that this balance shifts in favor of order – in favor of the government's ability to deal with conditions that threaten the national well-being.[1]

* * *

Everyone does not share Chief Justice Rehnquist's vision of the balance between liberty and order. The past several months have seen the growth of a new movement – call it the "anti-anti-terrorism" movement, if you will. The thesis of the movement, which has some of the appearances of a political campaign, is that steps being taken domestically to combat the potential for terrorist attacks are too intrusive and a threat to cherished civil liberties.

The principal focus of the campaign is the USA PATRIOT Act,[2] a law passed with overwhelming support in Congress immediately following the September 11th terrorist attacks.[3] Taking many

---

* Senior Legal Research Fellow, Center for Legal and Judicial Studies, The Heritage Foundation; Adjunct Professor of Law, George Mason University School of Law. Portions of this paper were presented at a debate on the Patriot Act hosted by the Federalist Society of Duquesne Law School, whom I thank for the opportunity to speak. I also thank Todd Gaziano, Rachel Brand, Dan Gallington, K. A. Taipale and Jim Dempsey for their contribution to my education on various matters discussed in this paper. They, of course, bear no responsibility for any errors that remain and, indeed, doubtless disagree with many of the conclusions drawn herein.

1. WILLIAM REHNQUIST, ALL THE LAWS BUT ONE: CIVIL LIBERTIES IN WARTIME 222 (1998).

2. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. 107-56, 115 Stat. 272 (Oct. 26, 2001).

3. Typical of the public criticism was the recent resolution of the National League of Cites, calling for repeal of various portions of the Patriot Act. *See* Audrey Hudson, *Cities in Revolt over Patriot Act*, WASH. TIMES, Jan. 5, 2004. A number of cities and municipalities have passed similar resolutions. *See, e.g,* Jessica Garrison, *L.A. Takes Stand Against Patriot Act*, L.A. TIMES, Jan. 22, 2004, at B4. Responding to these criticisms, President Bush has called for reauthorization of the Patriot Act. *See* State of the Union (Jan. 20, 2004) ("The terrorist threat will not expire on [a] schedule. Our law enforcement needs [the Patriot Act] to protect our citizens.").

forms, the campaign argues that various provisions of the Patriot Act, and related laws and practices, have greatly infringed upon American liberties, while failing to deal effectively with the threat of terror. Criticism of the anti-terrorist campaign is not, however, limited to the Patriot Act – many other aspects of the Bush Administration's domestic response to terrorism have come under fire. To some degree, the Patriot Act as conceived by the public is broader than its actual provisions. Its very name has come to serve as a symbol for all of the domestic anti-terrorist law enforcement actions. It has become, if you will, a convenient short hand formulation for all questions about the alteration in the balance between civil liberty and national security that have occurred since September 11th.

There are two over-arching themes that animate criticism of the Patriot Act (using the phrase now in the broad, symbolic sense already noted): First, critics of the Patriot Act frequently decry the expansion of executive authority in its own right. They, generically, equate the potential for abuse of Executive Branch authority with the existence of actual abuse. They argue, either implicitly or explicitly, that the growth in executive power is a threat, whether or not the power has, in fact, been misused in the days since the anti-terrorism campaign began. In essence, these critics come from a long tradition of limited government that fears any expansion of executive authority, notwithstanding the potential for benign and beneficial results, because they judge the potential for the abuse of power to outweigh the benefits gained.

The second theme of many criticisms of the Patriot Act and other government responses is one we might call a fear of technology. In service of our efforts to combat terrorism, the government has begun to explore ways of taking advantage of America's superior capacity to manage data through new information technologies. The Transportation Security Administration's proposal for a new computer-assisted passenger screening program (CAPPS II) is one such program.[4]

These new technologies offer two advantages over current investigative practices – they have the potential to both *expand* the ambit of the information available to federal law enforcement and intelligence agencies and to *enhance* the efficiency with which

4. CAPPS II stands for Computer-Assisted Passenger Prescreening System II. *See* 68 Fed. Reg. 45265 (Aug. 1, 2003) (describing program). The CAPPS II program is discussed in more detail in Section II of this paper.

those agencies are able to examine and correlate information already in their possession. And both possibilities raise corresponding fears among critics of the programs. Expanded access to information increases executive power. And with great efficiency comes more effective use of power. Thus, the hesitancy to use new technology, though sometimes born of technological apprehension, also resonates with the principal theme of critics, a reluctance to expand the capacity of the government to examine the lives of individuals.[5]

Criticism of the Patriot Act, however, sometimes misapprehends important distinctions. First, the criticism often blurs potential and actuality. To be sure, many aspects of the Patriot Act (and other governmental responses) do expand the power of the government to act. And Americans should be cautious about any expansion of government power, for assuredly such expansion admits of the *potential* for abuse. But by and large, the potential for abuse of new Executive powers has proven to be far less than critics of the Patriot Act have presumed it would be.[6]

---

5. A third theme underlying criticism of the Patriot Act is more clearly political. As is to be expected, criticism of the Bush Administration's response to terrorism has, inevitably, become a part of the political landscape. *See, e.g.*, MoveOn.org, *The Administration is Using Fear as a Political Tool*, N.Y. TIMES (Nov. 25, 2003) (full page ad reprinting excerpts of speech by former Vice President Al Gore). It is no coincidence that many Democratic presidential candidates garner great applause with the "novel" suggestion that, if elected, they will fire Attorney General Ashcroft. *E.g.* Carl Matzelle, *Gephardt Talks the Talk Steelworkers Want to Hear*, CLEVE. PLAIN DEALER, Dec. 7, 2003, at A24 (promise to fire Ashcroft "within first five seconds" of new administration); Greg Pierce, *Inside Politics*, WASH. TIMES, Sept. 23, 2003, at A6 (noting "frenzy" of "Ashcroft bashing"). To the extent that criticism of the Patriot Act and related activities is purely political, the debate over these truly difficult questions is diminished. Thoughtful criticism recognizes both the new realities of the post-September 11th world and the potential for both benefit and abuse in governmental activity.

6. The Inspector General for the Department of Justice has reported that there have been no instances in which the Patriot Act has been invoked to infringe on civil rights or civil liberties. *See* Report to Congress on Implementation of Section 1001 of the USA Patriot Act (Jan. 27, 2004); *see also Report Finds No Abuses of Patriot Act*, WASH. POST, Jan. 28, 2004, at A2. This is consistent with the conclusions of others. For example, at a Senate Judiciary Committee Hearing on the Patriot Act Senator Joseph Biden (D-DE) said that "some measure of the criticism [of the Patriot Act] is both misinformed and overblown." His colleague, Senator Dianne Feinstein (D-CA) said: "I have never had a single abuse of the Patriot Act reported to me. My staff . . . asked [the ACLU] for instances of actual abuses. They . . . said they had none." Even the lone Senator to vote against the Patriot Act, Russ Feingold (D-WI) said that he "supported 90 percent of the Patriot Act" and that there is "too much confusion and misinformation" about the Act. *See Senate Jud. Comm. Hrg.* 108th Cong, 1st Sess. (Oct. 21, 2003). These views, from Senators outside of the Administration and an internal watchdog, are at odds with the fears often expressed by the public.

Second, much of the belief in the potential for abuse stems from a misunderstanding to the true nature of the new powers that government has deployed to combat those threats. To a surprising degree, opposition to the executive response to terror is premised on a mistaken, and sometimes overly apocalyptic, depiction of the powers that have accrued to the government.

More fundamentally, those who fear the expansion of executive power in the war on terrorism offer a mistaken solution – prohibition. While we could afford that solution in the face of traditional criminal conduct, we cannot afford that answer in combating the threat of terror. In the context of current circumstances, vigilance and oversight, enforced through legal, organizational and technical means, are the answer to potential abuse – not prohibition. We must keep a watchful eye to control for the risk of excessive encroachment, but if we do, the likelihood of erosion of civil liberties can be substantially reduced.

This article addresses many of the conceptions and misconceptions attending the public debate on the threat to civil liberty from the expansion of executive power. Section I outlines some basic principles that should guide the analysis of the Patriot Act, and related expansions of government power. It summarizes some of the relevant history and attempts to identify relevant similarities and difference between past experiences and the contemporary situation. It then offers some basic principles for use in assessing the potential threat to civil liberties posed by various legal and technological changes. Section II then conducts a detailed analysis of some of these changes, acknowledging at several points that ambiguity and the potential for abuse exists, at others that real problems may arise, and arguing, at others, that criticisms of the Patriot Act have strayed away from reality and into a sort of mythology.[7]

7. The principal focus of this article is domestic law enforcement efforts under the Patriot Act and related changes in FBI investigative guidelines, as well as efforts by the Transportation Security Administration. Thus, though not exclusively focused on the provisions of the Act, the article's scope is narrow and leaves for analysis in other forums discussions of the legal aspects of military or quasi-military responses to terrorism such as the detention of "enemy combatants" in America or the detention of "unlawful combatants" at Guantanamo Bay. Though those actions can be analyzed using the same framework adopted by this article, they raise substantially distinct legal issues.

I. THE CONTEXT WITHIN WHICH WE ACT – THE CHANGING NATURE OF LAW ENFORCEMENT AND INTELLIGENCE ACTIVITY

To begin with, the analysis of the expansion of domestic efforts to combat the potential for terrorism needs to be placed in its appropriate context. To a very real degree, one's assessment of the Patriot Act rests upon that context – how one views the history of American responses in times of war, what one views as the constitutional constraints on the use of Executive power, and whether, in the end, one places the threat of terror into the "law enforcement" box, or the "intelligence" box for legal analysis. In this section, I examine some of this context, and begin making the argument that the war on terror is not a law enforcement problem in the classical sense, and thus, that most of the difficulties in analysis stem from trying to fit the square peg of law enforcement practices into the round hole of terrorist reality.

A. The Lessons Of History

As we consider the American response to terrorism and the use of executive power, many caution against repeating past excesses. They see, in history, a series of lessons about over-reactions in the face of war. In this vision, past responses to threats necessarily lead to good faith, but over-zealous response. The tension between civil liberty and national security is but one example of how we return to the same fundamental issues over and over again. Consider the following history:[8]

In 1798, the Napoleonic wars raged in Europe. President John Adams, a Federalist, effectively brought the United States into a state of undeclared war with France, on the side of the British. Thomas Jefferson and the Democratic Republican party opposed these measures as likely to provoke an unnecessary war. The Federalists, in turn, accused the Jeffersonians of treason.

---

8. This summary of the history is substantially derived from a lecture Professor Geoffrey Stone of the University of Chicago recently gave to the Supreme Court Historical Society. *See* Geoffrey Stone, *Civil Liberties in Wartime*, 28 J.S. CT. HIST. 215 (2003). This article provides a far more detailed summary and understanding of these historical events, and is the source of much of the historical information summarized below, though it reaches different conclusions regarding the lessons to be drawn from that history. *See also* Paul Rosenzweig, *Securing Freedom And The Nation: Collecting Intelligence Under The Law*, Testimony Before the United States House of Representatives, Permanent Select Committee on Intelligence (Apr. 9, 2003) (discussing lessons of history).

To exacerbate the situation, the Federalist Congress enacted the Alien and Sedition Acts of 1798.[9] The Alien Act authorized the president to deport any non-citizen he judged dangerous to the peace and safety of the United States, without a hearing or the right to present evidence. The Sedition Act prohibited the publication of false, scandalous and malicious writings against the government, the Congress or the president with intent to bring them into contempt or disrepute. These were, in effect, aggressive efforts to suppress political criticism of Adams, his policies, and his administration. The Act expired by its terms, and after Jefferson replaced Adams as President, he pardoned all those who were convicted under the act. Though never tested in the Supreme Court, these acts are widely regarded as having been unconstitutional and a stain on American liberty.

During the Civil War, President Abraham Lincoln suspended the writ of habeas corpus on eight occasions. The broadest such suspension declared that "all persons . . . guilty of any disloyal practice . . . shall be subject to court martial."[10] As many as 38,000 civilians were imprisoned by the military, in reliance on this authority.[11] In 1866, a year after the war ended, the Supreme Court ruled that the president was not constitutionally empowered to suspend the writ of habeas corpus, even in time of war, if the ordinary civil courts were functioning.[12] Here, again, the suspension is remembered by some as an excessive response to a crisis and has come to be regarded as an unfortunate wartime error.

In 1917, the United States entered World War I. During the war, federal authorities acting under the aegis of the Espionage Act[13] prosecuted more than 2,000 people for their opposition to the war. As a result, virtually all dissent with respect to the war was suppressed. Though the Supreme Court initially approved most federal actions in support of the war,[14] over the next half-century,

---

9. *See* An Act Concerning Aliens, 5th Cong., 2d Sess, 1 Stat 570-72; An Act Concerning Enemy Aliens, 5th Cong., 2d Sess., 1 Stat 577-78 (the Alien Acts); An Act for the Punishment of Certain Crimes Against the United States, 5th Cong., 2d Sess., 1 Stat. 596-97 (the Sedition Act).

10. ROY P. BALSER ET AL. EDS., THE COLLECTED WORKS OF ABRAHAM LINCOLN 436-37 (Rutgers Univ. Press 1953-55).

11. MARK E. NEELY, JR., THE FATE OF LIBERTY: ABRAHAM LINCOLN AND CIVIL LIBERTIES 113-38 (Oxford 1991); *see also* REHNQUIST, *supra* note 1, at 49-50 (estimating 13,000).

12. Ex parte Milligan, 71 U.S. 2 (1866).

13. Act of June 15, 1917, ch. 30, tit. I, § 3, 40 Stat. 219.

14. *E.g.*, Schenck v. U.S., 249 U.S. 47 (1919); Debs v. U.S., 249 U.S. 211 (1919).

the Court overruled every one of its World War I decisions, effectively repudiating the excess of that war-time era.[15]

Finally, and most notoriously, on Feb. 19, 1942, President Franklin Delano Roosevelt signed Executive Order 9066,[16] which authorized the Army to "designate military areas" from which "any persons may be excluded." Over the next eight months, more than 110,000 people of Japanese descent were forced to leave their homes in California, Washington, Oregon and Arizona. Though the Supreme Court upheld the president's action,[17] it has come to be recognized as a grave error. In 1988, President Ronald Reagan offered an official presidential apology and reparations to each of the Japanese-American internees.[18]

Some see in this history a cautionary note. As Professor Stone has said: "In time of war – or, more precisely, in time of national crisis – we respond too harshly in our restriction of civil liberties, and then, later regret our behavior."[19] And we should not disregard that caution.

But reading too much into this history is a mistake – potentially quite a grave one. First, and most obviously, it disregards the reality of necessity. As Justice Arthur Goldberg so famously said, "while the Constitution protects against invasions of individual rights, it is not a suicide pact."[20] And while some of these reactions were plainly over-reactions (nobody argues today that the internment of the Japanese served a useful military purpose), others were not.

Many, for example, think that Lincoln's suspension of the writ of habeas corpus was essential to the prosecution of the war.[21]

---

15. *E.g.*, Brandenburg v. Ohio, 395 U.S. 444 (1969).

16. 7 Fed. Reg. 1407 (1942).

17. *Korematsu v. United States*, 323 U.S. 214 (1944).

18. Civil Liberties Act of 1988, 102 Stat. 903, Pub. L. 100-383 (Aug. 10, 1988).

19. Stone, *supra* note 8, at 215.

20. Kennedy v. Mendoza-Martinez, 372 U.S. 144, 160 (1963). Justice Goldberg was quoting Justice Robert Jackson, who made the same observation in Terminnelo v. Chicago, 337 US. 1 (1949) (Jackson, J., dissenting).

> The choice is not between order and liberty. It is between liberty with order and anarchy without either. There is danger that, if the court does not temper its doctrinaire logic with a little practical wisdom, it will convert the constitutional Bill of Rights into a suicide pact.

Id. at 37 (Jackson, J., dissenting).

21. *E.g.*, HARRY V. JAFFA, A NEW BIRTH OF FREEDOM: ABRAHAM LINCOLN AND THE COMING OF THE CIVIL WAR 364 (Rowman & Littlefield Publishers Inc. 2000):

> There can hardly be any question but that the provision for suspending the writ of habeas corpus is placed in the Constitution to enable the government to provide for the public safety in the case of a rebellion. *Where* in the Constitution it is placed is

Some argue that it was necessary to protect the troops, save Maryland for the Union, and secure the safety of Washington, D.C.[22] Lincoln certainly felt the necessity.[23] And later in the war, the anti-draft riots in New York (made cinematically famous just a short while ago in "Gangs of New York") threatened to deprive the Union army of conscripts.[24] Had that happened (though, of course, a counter-factual can never be proven), Lincoln feared a premature end to the war – leaving the United States divided and slavery ongoing.[25] Using the authority granted him by Congress in the Habeas Corpus Act,[26] Lincoln directed the draft boards to ignore writs of habeas corpus issued to them by state courts seeking release of the conscripts.[27] It is not unreasonable to argue that, however *de jure* improper Lincoln's acts were, they were *de facto* a justified necessity that ought, in retrospect, to be praised.

The first lesson here is that we should not be too harsh in our retrospective judgments – hindsight is always 20/20. But as we live within the times and face the challenges of today, we must be at least a little generous in our self-review, for we will not know for many years whether or not our fears of today are well-founded.

---

wholly subordinate to why it is there at all. Lincoln's suspension of the writ is therefore lawful. Q.E.D.

Id.; William Rehnquist, *Civil Liberty and the Civil War*, GAUER LECTURE (NLCPI 1997).

> Lincoln felt that the great task of his administration was to preserve the Union . . . . [I]t is in the nature of the presidency during wartime to focus on accomplishment of . . . . strategic ends on an emergency basis without too much regard for any resulting breaches in the shield which the Constitution gives to civil liberties. Perhaps it may be best that the courts reserve serious consideration of questions of civil liberties . . . . until after the war is over.

Id. at 23.

22. *See* NEELY, *supra* note 11, at 29 ("Not every historian today would credit it [i.e. the suspension of habeas corpus] with saving Maryland for the Union, but that conclusion became almost a truism in Lincoln's day."); Rehnquist, "All the Laws But One" Online Newshour, Nov. 11, 1998, interview with Chief Justice Rehnquist, *available at* http://www.pbs.org/newshour/gergen/november98/gergen_11-11.html (Lincoln's suspension protected troop movements and Washington, D.C.).

23. Lincoln made the argument in a special address to Congress on July 4, 1861. *See* DON FEHRENBACHER, ED., SPEECHES AND WRITINGS: 1859-1865 246-62 (1989).

24. The draft riots have been called the greatest instance of domestic violence in United States history. *See* JAMES G. RANDALL & DAVID DONALD, THE CIVIL WAR AND RECONSTRUCTION 361 (2d ed. 1961). They were no trivial threat to the Union's ability to wage war successfully.

25. NEELY, *supra* note 11, at 69-70 (quoting HOWARD K. BEALE, ED., THE DIARY OF EDWARD BATES, 1859-1866 306 (Gov't. Printing Off. 1933).

26. An Act relating to Habeas Corpus, and regulating Judicial Proceedings in Certain Cases, ch. 81, § 1, 12 Stat. 755, 755 (1863).

27. The relevant text of the proclamation (issued on September 15, 1863), which suspended the writ nationwide in cases involving draftees and deserters, is reprinted in NEELY, *supra* note 11, at 72 (quoting BALSER ET AL., *supra* note 10, at 460).

B. Contemporary Oversight

Indeed, by comparison with past excesses, this history should actually give us some comfort. Many who are concerned with current activities think that we are on a downward spiral towards diminished civil liberties. But a better view of this history shows that the balance between liberty and security is more like a pendulum that gets pushed off-center by significant events (such as those of September 11th) than a spiral. Over time, after Americans have recovered from the understandable human reaction to catastrophe and after the threat recedes, the pendulum returns to center.

We should acknowledge the historical reality that when the wartime crisis passes, the balance swings back in favor of freedom and liberty. And since World War II, our society has matured such that the scope of the swing in the pendulum is not nearly as great as it had been in the past. Whatever one may think of the detention of three Americans as enemy combatants, for example, there can be little disagreement that the detention of three Americans (whose detention is based upon some quantum of individualized suspicion), is sufficiently different in degree from the wholesale detention of over 100,000 Japanese-Americans (whose detention was ordered in the complete absence of any individualized suspicion) as to be different in kind.[28] To quote Chief Justice Rehnquist:

> [T]here is every reason to think that the historic trend against the least justified of the curtailments of civil liberty in wartime will continue in the future. It is neither desirable nor is it remotely likely that civil liberty will occupy as favored a position in wartime as it does in peacetime. But it is both desirable and likely that more careful attention will be paid by the courts to the basis for the government's claims of necessity as a basis for curtailing civil liberty.[29]

What accounts for this seeming change in contemporary context? Though little empirical evidence exists, a rough analysis can

---

28. *See* Michael Chertoff, *Law, Loyalty, and Terror*, THE WKLY. STANDARD 15, 16 (Dec. 1, 2003) (In response to September 11, "the government quite self-consciously avoided the kinds of harsh measures common in previous wars.").

29. REHNQUIST, *supra* note 1, at 224-25. Or, as Jeffrey Rosen has written: "[N]one of the legal excesses that followed 9/11 could compare to those that followed World War I." JEFFREY ROSEN, THE NAKED CROWD 131 (Random House 2004).

identify a number of factors, all of which contribute to greater oversight in the exercise of executive authority, constraining the greatest excesses. These factors would include:

- A more activist court that is far more willing to overturn executive branch action, acting as a limit on excessive power. Earlier times of crisis all occurred before the so-called "rights revolution" of the 1960s and the growth of judicial power. Indeed, the current Rehnquist Court has invalidated more acts of Congress than any previous court,[30] exhibiting a high degree of involvement in curtailing authority.[31]

- A more partisan Congress. Though sometimes seen as a bad thing, the growth of partisanship has created at least one positive benefit – a growth in the "market" for oversight of the executive branch. Since the Watergate era, we have seen an increasing use of Congressional investigative authority – sometimes for good, and sometimes for ill. But the prospect of aggressive Congressional oversight acts as a check on executive power, as even the prospect of public censure has the *in terrorem* effect of preventing abuse.

- The growth of investigative journalism. Clearly, this is another change that has some potential adverse consequences. But few can deny that post-Watergate, the press has come to more aggressively serve an important public function, exposing activities that some might otherwise prefer to keep secret. None can imagine a return to the days when the press actively participated in concealing Roosevelt's injuries, or Kennedy's dalliances. And that means, equally, that the prospect of secret prosecutions and secret searches and seizures is minimal, at best.

---

30. Remarks, Akhil Reed Amar, The Heritage Foundation (July 9, 2002); *cf.* Cass Sunstein, *A Hand in the Matter*, LEGAL AFF. (Mar./Apr. 2003) (noting that the Rehnquist Court has struck down 26 Acts of Congress since 1995).

31. The Supreme Court has yet to accept any cases directly arising from the Patriot Act. However, the Court's recent decision to hear both the "enemy combatants cases," *see* Hamdi v. Rumsfeld, 337 F.3d 335 (4th Cir. 2003), *cert. granted*, 124 S. Ct. 981 (2004); Padillia v. Rumsfeld, 352 F.3d 695 (2d Cir. 2003), *cert. granted*, 124 S. Ct. 1353 (2004), and the "Guantanamo detainees case," *see* Al Odah v. U.S., 321 F.3d 1134 (D.C. Cir. 2003), *cert. granted*, 124 S. Ct. 534 (2003) (consolidated with *Rasul v. Bush*), reflects this activism and the involvement of the Court at a very early stage of the war – far earlier than in past conflicts. *E.g.*, Ex parte Milligan, 71 U.S. 2 (1866) (decision rendered one year after hostilities ended in Civil War).

- The rise of the public interest groups. In no other time did Americans organize themselves into public interest groups in the way they do now. No other era saw the existence, for example, of numerous public interest litigation groups like the ACLU. These organizations, through their public information and litigation activities, act as an important check on the exercise of executive authority. They are, in effect, the "canary in the mineshaft," serving as an early warning system of abuse.[32]

- The increase in the public's ability to monitor government. Though technology, assuredly, offers greater opportunity for our government to monitor our activities, that same technology holds the promise of greater public accountability by enhancing the transparency of government functions.[33]

- And, finally, the public is far more educated about civil liberties today than, seemingly at any time in the past. With the rise of the Information Age and the internet, we are far more able to individually gather information necessary to make decisions and to organize a response to government power if one is deemed necessary. From the Ozzie and Harriet quiet of suburbia in the 1950's, we have come to a point where many Americans are vitally concerned about freedom, liberty, and government action and exercise their franchise with those concerns in mind.[34]

As noted, there is little more than anecdotal evidence to support this analysis – yet it has the appeal of both common sense and consistency with contemporary experience. It appears that we have strengthened, substantially, our ability to examine, oversee, and correct, abuses of executive power. The public is in a stronger

---

32. *See* Michael Kinsley, *An Incipient Loss of Freedom*, WASH. POST, June 15, 2003, at B07 ("The American Civil Liberties Union is alarmed, but the ACLU's function, which I admire and support, is to be alarmed before I am, like the canary down the mineshaft.").

33. *See generally* DENNIS BAILEY, THE OPEN SOCIETY PARADOX: WHY THE TWENTY-FIRST CENTURY CALLS FOR MORE OPENNESS NOT LESS (Brassey 2004) (forthcoming); *See* DAVID BRIN, THE TRANSPARENT SOCIETY (1999).

34. Survey evidence supports the instinct that the public is reacting cautiously. Though immediately after September 11th, 60% agreed that the average citizen would have to give up civil liberties to fight terrorism, by June 2002 that number had fallen to 46%. *See* Amatai Etzioni & Deidre Mead, *The State of Society – a Rush to Pre-9/11, available at* http://www.gwu.edu/~ccps/The_State_of_Society.html. One suspects the number has fallen still further in the subsequent months.

position today than it ever has been before. And that power of oversight gives us freedom – freedom to grant the government great powers when the need arises, secure in the knowledge that we can restrain their exercise appropriately. In short, one possible lesson from history is that we should not be utterly unwilling to adjust our response liberty and security in today's crisis of terrorism – for we have the capacity to mange that adjustment, and readjust it as necessary.[35]

C. The Constitutional Structure

While a large fraction of the debate over new law enforcement and intelligence systems focuses on perceived intrusions on civil liberties, Americans should keep in mind that the Constitution weighs heavily on both sides of the debate over national security and civil liberties. The President and Congressional policymakers must respect and defend the individual civil liberties guaranteed in the Constitution when they act, but there is also no doubt that they cannot fail to act when we face a serious threat from a foreign enemy.

The Preamble to the Constitution acknowledges that the United States government was established in part to provide for the common defense. The war powers were granted to Congress and the President with the solemn expectation that they would be used. Congress was also granted the power to "punish ... Offenses against the Law of Nations," which include the international law of war, or terrorism.[36] In addition, serving as chief executive and commander in chief, the President also has the duty to "take Care that the Laws be faithfully executed," including vigorously enforcing the national security and immigration laws.

Thus, as we assess questions of civil liberty it important that we not lose sight of the underlying end of government – personal and national security. That balance is not a zero-sum game, by any means. But it is vital that we not disregard the significant factors weighing on *both* sides of the scales.

---

35. The foregoing list identifies sociological factors that will allow for enhanced oversight. There are likely to be technological factors as well. We can readily imagine a strong audit function that records all use of new investigative techniques and, thus, enables us to readily identify and punish abuse of the system. *See, e.g,* K. A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 2 (2003) (arguing for utility of strong audit technology) (*available at* http://www.stlr.org/cite.cgi?volume=5&article=2).

36. U.S. CONST. art. I, § 8.

Contemporary, Constitutional limitations have little to add to this equation.[37] Under settled modern Fourth Amendment jurisprudence, law enforcement may secure without a warrant (through a subpoena) an individual's bank records, telephone toll records, and credit card records, to name just three of many sources of data. Other information in government databases (e.g. arrest records, entries to and exits from the country, and driver's licenses) may be accessed directly without even the need for a subpoena.

In 1967, the Supreme Court said that the Fourth Amendment protects only those things in which someone has a "reasonable expectation of privacy" and, concurrently, that anything one exposes to the public (i.e., places in public view or gives to others outside of his own personal domain) is not something in which he has a "reasonable" expectation of privacy—that is, a legally enforceable right to prohibit others from accessing or using what one has exposed.[38] So, for example, federal agents need no warrant, no subpoena, and no court authorization to:

- have a cooperating witness tape a conversation with a third party (because the third party has exposed his words to the public);[39]
- attach a beeper to someone's car to track it (because the car's movements are exposed to the public);[40]
- fly a helicopter over a house to see what can be seen;[41] or
- search someone's garbage.[42]

37. *See, e.g.*, Paul Rosenzweig & Michael Scardaville, *The Need to Protect Civil Liberties While Combating Terrorism: Legal Principles and the Total Information Awareness Program*, LEGAL MEMORANDUM NO. 6, at 12-13 (The Heritage Foundation February 2003); Paul Rosenzweig, *Anti-Terrorism Investigations And The Fourth Amendment After September 11: Where And When Can The Government Go To Prevent Terrorist Attacks?*, Testimony Before the United States House of Representatives, Committee on the Judiciary, Subcommittee on the Constitution (May 20, 2003).

38. Katz v. U.S., 389 U.S. 347 (1967).

39. U.S. v. White, 401 U.S. 745 (1971). A few states have consent laws that restrict the ability of state law enforcement officials to conduct taping of telephone conversations without consent.

40. U.S. v. Karo, 468 U.S. 705 (1984).

41. Florida v. Riley, 488 U.S. 445 (1989) (plurality opinion).

42. California v. Greenwood, 486 U.S. 35 (1988).

Thus, an individual's banking activity, credit card purchases, flight itineraries, and charitable donations are information that the government may access because the individual has voluntarily provided it to a third-party.[43] According to the Supreme Court, no one has any constitutionally based enforceable expectation of privacy in them. The individual who is the original source of this information cannot complain when another entity gives it to the government. Nor does he have a Constitutional right to notice of the inquiry.[44] Some thoughtful scholars have criticized this line of cases, but it has been fairly well settled for decades.[45]

Congress, of course, may augment the protections that the Constitution provides and it has with respect to certain information. There are privacy laws restricting the dissemination of data held by banks, credit companies, and the like.[46] But in almost all of these laws (the Census being a notable exception),[47] the privacy protections are good only as against other private parties; they yield to criminal, national security, and foreign intelligence investigations.

One important caveat should be made here – in the foregoing discussion we have identified principally the restrictions that apply to domestic law enforcement officials. Important additional restrictions continue to exist on the authority of foreign intelligence agencies to conduct surveillance or examine the conduct of American citizens. Conversely, however, the courts have recognized that in the national security context, the requirements of

---

43. The same is true of the physical characteristics that one exposes to the public every day. Many have ridiculed a research proposal to develop a means of identifying people from their physical characteristics, deriding it as the "Ministry of Silly Walks." Others fear such a capacity. But the government already has the authority and the capacity to identify an individual by surveillance photographs whenever he or she walks out the front door. (They may not, however, use technology to penetrate that door. Kyllo v. U.S., 533 U.S. 27 (2001)). From a legal perspective, the "better telephoto lens" proposed is not off limits.

44. SEC v. O'Brien, 467 U.S. 735 (1984). The lack of entitlement to notice flows, according to the Court, from the individual's abandonment of a claim of privacy arising from conveying the information to a third party. *Id.* at 743 (*citing U.S. v. Miller*, 425 U.S. 435, 443 (1973)).

45. *E.g.*, James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65 (1997).

46. *E.g.*, 12 U.S.C. §§ 3402, 3403 (bank disclosure); *id.* § 3407 (subpoenas to bank).

47. *E.g.*, 13 U.S.C. §§ 8, 9 (prohibition on disclosure of Census data); *id.* § 214 (penalties for disclosure). Recent reports claiming that Census data has been used to test the new CAPPS II algorithm, *see* Drew Clark, *The Outcry Over Airline Passenger Records*, NAT'L J. TECH. DAILY (Jan. 26, 2004), have been categorically denied by the Census Bureau. *See* Letter, Jefferson D. Taylor, Chief, Cong. Affairs Office, to Hon. Adam Putnam (Jan. 23, 2004).

the Fourth Amendment apply somewhat differently than they do in the context of domestic law enforcement.[48]

D. Type I and Type II Errors – The Reality of Terrorism

The full extent of the terrorist threat to America cannot be fully known.[49] Consider, as an example, one domestic aspect of that threat—an effort to determine precisely how many al-Qaeda operatives are in the United States at this time and to identify those who may enter in the future.

Terrorism remains a potent threat to international security. The U.S. State Department has a list of over 100,000 names worldwide of suspected terrorists or people with contact to terrorists.[50] Before their camps in Afghanistan were shut down, Al Qaeda trained at least 70,000 people and possibly tens of thousands more.[51] Al Qaeda linked Jemaah Islamiyah in Indonesia is estimated to have 3,000 members across Southeast Asia and is still growing larger.[52] Although the estimates of the number of al-Qaeda terrorists in the United States have varied since the initial attack on September 11, the figure provided by the government in recent, supposedly confidential, briefings to policymakers is 5,000.[53] This 5,000-person estimate may include many who are engaged in fundraising for terrorist organizations and others who were trained in some fashion to engage in jihad, whether or not they are actively engaged in a terrorist cell at this time. But these

---

48. Important restrictions continue to exist on the authority of foreign intelligence agencies to conduct surveillance or examine the conduct of American citizens. *E.g.*, Exec. Order No. 12333, 3 C.F.R. 200 (1982), *reprinted at* 50 U.S.C. § 401 note; Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (Apr. 1983) (National Academy of Science, *Legal Standards for the Intelligence Community in Conducting Electronic Surveillance* (Feb. 2000), *available at* http://www.fas.org/irp/nsa/standards.html) . However, as stated above, the courts have recognized that in the national security context, the requirements of the Fourth Amendment apply somewhat differently than they do in the context of domestic law enforcement. *See* U.S. v. U.S. Dist. Ct. (Keith), 407 U.S. 297 (1972) (applying Fourth Amendment in context of domestic national security surveillance); In re Sealed Case, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002) (applying Fourth Amendment in context of foreign intelligence surveillance).

49. This discussion is taken from Rosenzweig & Scardaville, *supra* note 37, at 5-6.

50. Eric Lichtblau, Administration Creates Center for Master Terror "Watch List," N.Y. TIMES, Sept. 17, 2003.

51. During an interview on NBC's Meet the Press, U.S. Senator Bob Graham was quoted as saying, ". . . al-Qaeda has trained between 70,000 and 120,000 persons in the skills and arts of terrorism . " *Meet the Press* (NBC television broadcast, July 13, 2003).

52. Terence Hunt, *Bush Shows Resolve by Visiting Bali*, Chi. Sun-Times, Oct. 22, 2003, at 36.

53. Bill Gertz, *5,000 in U.S. Suspected of Ties to al Qaeda*, WASH. TIMES, July 11, 2002.

and other publicly available statistics support two conclusions: (1) no one can say with much certainty how many terrorists are living in the United States; and (2) many who want to enter in the foreseeable future will be able to do so.

Understanding the scope of the problem demonstrates the difficulty of assessing the true extent of the risk to the United States. Consider this revealing statistic: "[M]ore than 500 million people [are] admitted into the United States [annually], of which 330 million are non-citizens."[54] Of these:

- Tens of millions arrive by plane and pass through immigration control stations, often with little or no examination.[55]

- 11.2 million trucks enter the United States each year.[56] Many more cars do so as well; more than 8.5 million cars cross the Buffalo–Niagara bridges each year alone, and only about 1 percent of them are inspected.[57]

- According to the Department of Commerce, approximately 51 million foreigners vacationed in the United States last year, and this figure is expected to increase to 61 million in three years.[58]

- There are currently approximately 11 million illegal aliens living in the United States. Roughly 5 million entered legally and simply overstayed their lawful visit.[59]

- Over half a million foreign students are enrolled in American colleges, representing roughly 3.9 percent of total enrollment, including:

  1. 8,644 students from Pakistan.

---

54. White House, *Securing America's Borders Fact Sheet*, *available at* www.whitehouse.gov (last accessed Jan. 14, 2003).

55. Office of Travel and Tourism Industries, *Inbound Travel to the U.S.*, U.S. Dept. of Commerce, *available at* http://tinet.ita.doc.gov/outreachpages/inbound.general_information.inbound_overview.html?ti_cart_ cookie=20030127.125013.04230.

56. White House, *supra* note 54.

57. MICHELLE MALKIN, INVASION: HOW AMERICA STILL WELCOMES TERRORISTS, CRIMINALS, AND OTHER FOREIGN MENACES TO OUR SHORE 8 (Regnery Publishing Inc., 2002).

58. Office of Travel and Tourism Industries, *supra* note 55.

59. MALKIN, *supra* note 57, at xii, 197.

> 2. A total of 38,545 students from the Middle East, including 2,216 from Iran, 5,579 from Saudi Arabia, and 2,435 from Lebanon, where Hezballah and other terrorist organizations train.
>
> 3. About 40,000 additional students from North African, Central and Southeast Asian nations where al-Qaeda and other radical Islamic organizations have a strong presence.[60]

To be sure, not all of these visitors pose a risk – but their sheer volume demonstrates the scope of the potential risk that some within this group do pose.

And, of course, the threat is not exclusively internal. The newest terrorist target may be global shipping. The world is particularly vulnerable to maritime terrorism and maritime piracy is growing increasingly rampant.[61] Lloyd's List has reported that terrorists might be training maritime pilots in the Malacca Straits in order to capture a ship, pilot it into a port or chokepoint and detonate it.[62]

This illustrates the other part of the story. The danger to America posed by terrorists arises from the new and unique nature of potential acts of war. Virtually every terrorism expert in and out of government believes there is a significant risk of another attack. Unlike during the Cold War, the threat of such an attack is asymmetric. In the Cold War era, U.S. analysts assessed Soviet capabilities, thinking that their limitations bounded the nature of the threat the Soviets posed. Because of the terrorists' skillful use of low-tech capabilities (e.g. box cutters), their capacity for harm is essentially limitless. The United States therefore faces the far more difficult task of discerning their intentions. Where the Soviets created "things" that could be observed, the terrorists create only transactions that can be sifted from the noise of everyday activity only with great difficulty. It is a problem of unprecedented scope, and one whose solution is imperative if American lives are to be saved.

As should be clear from the outline of the scope of the problem, the suppression of terrorism will not be accomplished by military

---

60. Institute of International Education, *Open Doors*, *available at* http://opendoors.iienetwork.org.

61. *See, e.g.*, William Langewische, *Anarchy at Sea*, THE ATLANTIC (Sept. 2003).

62. Lloyd's List International, *Asia Pirates Training for Terrorist Attack*, Oct. 15, 2003.

means alone. Rather, effective law enforcement and/or intelligence gathering activity are the key to avoiding new terrorist acts. Recent history supports this conclusion.[63] In fact, police have arrested more terrorists than military operations have captured or killed. Police in more than 100 countries have arrested more than 3000 Al Qaeda linked suspects,[64] while the military captured some 650 enemy combatants.[65] Equally important, it is policing of a different form – preventative rather than reactive, since there is less value in punishing terrorists after the fact when, in some instances, they are willing to perish in the attack.

The foregoing understanding of the nature of the threat from terrorism helps to explain why the traditional law enforcement paradigm needs to be modified (or, in some instances, discarded) in the context of terrorism investigations. The traditional law enforcement model is highly protective of civil liberty in preference to physical security. All lawyers have heard one or another form of the maxim that "it is better that 10 guilty go free than that 1 innocent be mistakenly punished."[66] This embodies a fundamentally moral judgment that when it comes to enforcing criminal law, American society, in effect, prefers to have many more Type II errors (false negatives) than it does Type I errors (false positives).[67] That preference arises from two interrelated grounds: one is the historical distrust of government that, as already noted, animates many critics of the Patriot Act. But the other is, at least implicitly, a comparative valuation of the social costs attending the two types of error. We value liberty sufficiently highly that we see a great cost in any Type I error. And, though we realize that Type II errors free the guilty to return to the general population, thereby imposing additional social costs on society, we have a common sense understanding that those costs, while significant,

---

63. *See, e.g.*, Dana Dillon, *War on Terrorism in Southeast Asia: Developing Law Enforcement*, BACKGROUNDER NO. 1720 (Heritage Foundation Jan. 22, 2004).

64. Peter Slevin, *U.S. Pledges Not to Torture Terror Suspects*, WASH. POST, June 27, 2003, at A01.

65. Francis Taylor, *Transcript: State Dept Official Says War Against Terrorism Continues*, June 9, 2003, *available at* http://usembassy.state.gov/tokyo/wwwh20030611a6.html.

66. *E.g.*, Furman v. Georgia, 408 U.S. 238, 367 n.158 (1972) (Marshall, J., concurring). The aphorism has its source in 4 BLACKSTONE, COMMENTARIES, ch. 27, at 358 (Wait & Co. 1907).

67. "In a criminal case . . . we do not view the social disutility of convicting an innocent man as equivalent to the disutility of acquitting someone who is guilty . . . . [T]he reasonable doubt standard is bottomed on a fundamental value determination of our society that it is far worse to convict an innocent man than to let a guilty man go free." In re: Winship, 397 U.S. 357, 372 (1970) (Harlan, J., concurring).

are not so substantial that they threaten large numbers of citizens or core structural aspects of the American polity.

The post-September 11th world changes this calculus in two ways. First, and most obviously, it changes the cost of the Type II errors. Whatever the cost of freeing John Gotti or John Muhammed might be, they are substantially less then the potentially horrific costs of failing to stop the next al-Qaeda assault. Thus, the theoretical rights-protective construct under which our law enforcement system operates must, of necessity, be modified to meet the new reality. We simply cannot afford a rule that "better 10 terrorists go free than that 1 innocent be mistakenly punished."[68]

Second, and less obviously, it changes the nature of the Type I errors that must be considered. In the traditional law enforcement paradigm, the liberty interest at stake is personal liberty – that is, freedom from the unjustified application of governmental force. We have as a model, the concept of an arrest, the seizure of physical evidence, or the search of a tangible place. As we move into the information age, and deploy new technology to assist in tracking terrorists, that model is no longer wholly valid.

Rather, we now add related, but distinct conception of liberty to the equation – the liberty that comes from anonymity.[69] Anonymity is a different, and possibly weaker, form of liberty: The American understanding of liberty interests necessarily acknowledges that the personal data of those who have not committed any criminal offense can be collected for legitimate governmental purposes. Typically, outside the criminal context, such collection is done in the aggregate and under a general promise that uniquely identifying individual information will not be disclosed. Think, for example, of the Census data collected in the aggregate and never disclosed, or of the IRS tax data collected on an individual basis, reported publicly in the aggregate, and only disclosed outside of

68. The closely related point, of course, is that we must guard against "mission creep." Since the justification for altering the traditional assessment of comparative risks is in part based upon the altered nature of the terrorist threat, we cannot alter that assessment and then apply it in the traditional contexts. *See* Rosenzweig & Scardaville, *supra* note 37, at 10-11 (arguing for use of new technology only to combat terrorism); William Stuntz, *Local Policing After the Terror*, 111 YALE L.J. 2137, 2183-84 (2002) (arguing for use of information sharing only to combat most serious offenses).

69. *See* Phillip Kurland, *The private I*, U. CHI. MAG., Autumn 1976, at 8 (characterizing three facets of privacy, broadly characterized as anonymity, secrecy, and autonomy) (quoted in Whalen v. Roe, 429 U.S. 589, 599 n.24 (1977)).

the IRS with the approval of a federal judge based upon a showing of need.[70]

What these examples demonstrate is not so much that our conception of liberty is based upon absolute privacy expectations,[71] but rather that government impingement on our liberty will occur only with good cause. In the context of a criminal or terror investigation, we expect that the spotlight of scrutiny will not turn upon us individually without some very good reason.

This conception of the liberty interest at stake (the interest that will be lost when Type I errors occur) also emphasizes one other point about privacy – in many ways the implementation of new laws and systems to combat terror are not an unalloyed diminution of privacy. Rather, the laws and practices can substitute one privacy intrusion (for example, a search of electronic data about an individual) for another privacy intrusion (the physical intrusiveness of body searches at airports). But this means that legal analysts cannot make broad value judgments – each person weighs the utility of their own privacy by a different metric. For many Americans, the price of a little less electronic privacy might not be too great if it resulted in a little more physical privacy – for others the opposite result might hold. This suggests little in resolving the tension, save that it cautions against allowing the tension to be resolved by unrepresentative institutions like the courts and in favor of allowing more representative institutions, like the legislature, to do their best at evaluating the multi-variable privacy preferences of the population.

Finally, it bears noting that not all solutions necessarily trade off Type I and Type II errors, and certainly not in equal measure. Some novel approaches to combating terrorism might, through technology, actually reduce the incidence of both types of error.[72] More commonly, we will alter both values but the comparative changes will be the important factor. Where many critics of the Patriot Act and other governmental initiatives go wrong is, it seems to me, in their absolutism – they refuse to admit of the possibility that we might need to accept an increase in the number of Type I errors. But that simply cannot be right – liberty is not an

70. *E.g.*, 26 U.S.C. § 7213 (prohibiting disclosure of tax information except as authorized for criminal or civil investigations).

71. *But cf.* Lawrence v. Texas, 123 S. Ct. 2472 (2003) (recognizing that certain intrusions into individual privacy are beyond governmental power).

72. *See* Taipale, *supra* note 35, at 31 (discussing use of ensemble classifiers to reduce error rates).

absolute value, it depends on security (both personal and national) for its exercise. As Thomas Powers has written: "In a liberal republic, liberty presupposes security; the point of security is liberty."[73] The growth in danger from Type II errors necessitates altering our tolerance for Type I errors. More fundamentally, our goal should be to minimize both sorts of errors.

E. Some General Principles

Of course, just because the Congress and the President have a constitutional obligation to act forcefully to safeguard Americans against attacks by foreign powers does not mean that every means by which they might attempt to act is necessarily prudent or within their power. Considering the foregoing analysis, core American principles would seem to require that any new counter-terrorism technology (deployed domestically) should be developed only within the following bounds:[74]

- No fundamental liberty guaranteed by the Constitution can be breached or infringed upon.

- Any increased intrusion on American privacy interests must be justified through an understanding of the particular nature, significance, and severity of the threat being addressed by the program. The less significant the threat, the less justified the intrusion.

- Any new intrusion must be justified by a demonstration of its effectiveness in diminishing the threat. If the new system works poorly by, for example, creating a large number of false positives, it is suspect. Conversely, if there is a close "fit" between the technology and the threat (that is, for example, if it is accurate and useful in predicting or thwarting terror), the technology should be more willingly embraced.

---

73. Thomas Powers, *Can We Be Secure and Free?*, THE PUB. INT. (Spring 2003).

74. These principles were first published in Paul Rosenzweig, Principles for Safeguarding Civil Liberties in an Age of Terrorism, EXECUTIVE MEMORANDUM NO. 854 (The Heritage Foundation, Jan. 2003).

- The full extent and nature of the intrusion worked by the system must be understood and appropriately limited. Not all intrusions are justified simply because they are effective. Strip searches at airports would prevent people from boarding planes with weapons, but at too high a cost.

- Whatever the justification for the intrusion, if there are less intrusive means of achieving the same end at a reasonably comparable cost, the less intrusive means ought to be preferred. There is no reason to erode Americans' privacy when equivalent results can be achieved without doing so.

- Any new system developed and implemented must be designed to be tolerable in the long term. The war against terror, uniquely, is one with no immediately foreseeable end. Thus, excessive intrusions may not be justified as emergency measures that will lapse upon the termination of hostilities. Policymakers must be restrained in their actions; Americans might have to live with their consequences for a long time.

From these general principles can be derived certain other more concrete conclusions regarding the development and construction of any new technology:

- No new system should alter or contravene existing legal restrictions on the government's ability to access data about private individuals. Any new system should mirror and implement existing legal limitations on domestic or foreign activity, depending upon its sphere of operation.

- Similarly, no new system should alter or contravene existing operational system limitations. Development of new technology is not a basis for authorizing new government powers or new government capabilities. Any such expansion should be independently justified.

- No new system that materially affects citizens' privacy should be developed without specific authorization by the American people's representatives in Congress and without provisions for their oversight of the operation of the system.

- Any new system should be, to the maximum extent practical, tamper-proof. To the extent the prevention of abuse is impossible, any new system should have built-in safeguards to ensure that abuse is both evident and traceable.

- Similarly, any new system should, to the maximum extent practical, be developed in a manner that incorporates technological improvements in the protection of American civil liberties.

- Finally, no new system should be implemented without the full panoply of protections against its abuse. As James Madison told the Virginia ratifying convention: "There are more instances of the abridgment of the freedom of the people by gradual and silent encroachments of those in power than by violent and sudden usurpations."[75]

These theoretical considerations and operational guidelines, while useful in constructing an *ex ante* heuristic for assessing new programs and law, are only of real value in application to concrete problems and proposed solutions. It is not enough to condemn every governmental initiative. Nor is it apt to afford the government a blank check for all actions designed to repel terror. Rather, each program and proposal must be carefully assessed on its own individual merits. Measured against these standards, the Patriot Act, and related governmental programs hold up fairly well – by and large they are of little practical threat to civil liberty and they hold the promise of significant benefit.

II. THE PATRIOT ACT AND OTHER INITIATIVES – WHAT IS MYTH AND WHAT IS REALITY?

Because specifics matter, it is not useful to generalize about various aspects of the Patriot Act (using the phrase now in a more focused sense). Some of the areas in which the law and policy have changed in the past 2 years are absolutely vital. In others, the potential for abuse is real, but the fears of abuse are overblown. In still others, there is cause for real concern. Each exercise of enhanced executive authority must be taken on its own

75. Speech to the Virginia Ratifying Convention, June 16, 1788, *reprinted in* Matthew Spalding, ed., THE FOUNDERS' ALMANAC 133 (The Heritage Foundation, 2002).

terms and merits. To a large degree, despite the popular view of the Patriot Act as a single unitary enactment, the various provisions can only be judged independently.

A. The Necessity of the Patriot Act – Information Sharing

The broadest criticism of the Patriot Act is that it was unnecessary – that it has added nothing to the efforts to avoid additional terrorist activities and that it is little more than a compilation of a "wish list" of law enforcement powers. This view, however, lacks persuasive force.

In particular, one aspect of the Patriot Act, embodied in Sections 202 and 218, was absolutely vital. Section 202 permits law enforcement information gathered under the aegis of a grand jury investigation to be shared with intelligence agencies. Section 218 allows the use of intelligence information gathering mechanisms, whenever the gathering of intelligence information is a "significant" purpose of the investigation and allows the information gathered to be shared with law enforcement. Taken together, these two sections, in effect, tear down an artificial "wall" that existed between law enforcement and intelligence agencies and permit their cooperation.[76]

Prior to the Patriot Act, a very real wall existed. It was derived from an earlier standard, requiring the use of intelligence-gathering mechanisms only when foreign intelligence was the

---

76. Some critics decry even this modest change. The ACLU has argued against the easing of grand jury restrictions: "While some sharing of information may be appropriate in some limited circumstances, it should only be done with strict safeguards . . . . The bill lacks all of these safeguards. As a result it may lead to the very abuses that the Church Committee exposed decades ago." ACLU, *How the USA-Patriot Act Puts the CIA Back in the Business of Spying on Americans*, Oct. 23, 2001, *available at* http://archive.aclu.org/congess/1102301j.html. It has also decried the expansion of authority to use the intelligence gathering authority of the FISA court: "It permits the FBI to conduct a secret search or to secretly record telephone conversations for the purpose of investigating crime even though the FBI does not have probable cause of crime. The section authorizes unconstitutional activity – searches and wiretaps in non-emergency circumstances – for criminal activity with no showing of probable cause of crime." *See* ACLU, *How the USA-Patriot Act Enables Law Enforcement to Use Intelligence Authorities to Circumvent the Privacy Protections Afforded in Criminal Cases*, Oct. 23, 2001, *available at* http://archive.aclu.org/congress/102301i.html.

Opposition to information sharing is not new and not limited to the ACLU. In 2000, responding to the concerns of the National Commission on Terrorism, Senator Jon Kyl proposed a discretionary information sharing regime. *See* Kyl Amdt. to S. 2507, § 610 (106th Cong. 2d Sess.) (proposing to allow disclosure of information by law enforcement agents to intelligence agents). The Department of Justice opposed this amendment. *See* Letter, Robert Raben, Asst. Atty. General to Sen. Jon Kyl (Sept. 28, 2000).

"primary purpose" of the activity.[77] This old "primary purpose" standard derived from a number of court decisions.[78] That standard was formally established in written Department guidelines in July 1995.[79] While information could be "thrown over the wall" from intelligence officials to prosecutors, the decision to do so always rested with national-security personnel – even though law-enforcement agents are in a better position to determine what evidence is pertinent to their case. The old legal rules discouraged coordination, and created what the Foreign Intelligence Surveillance Court of Review calls "perverse organizational incentives."[80]

The wall had some very negative real-world consequences. Former Department of Justice official Victoria Toensing tells of one:[81] In the 1980's, terrorists hijacked an airplane, TWA Flight 847, which eventually landed in Lebanon. At the time that negotiations were ongoing, the FBI had the capacity (pursuant to a FISA warrant) to intercept the communications between the hijackers on the plane and certain individuals in America. Negotiations did not, however, advance quickly enough and the terrorists killed an American, Robert Stethem, and graphically dumped his body onto the airport tarmac on live TV. The Department of Justice, as a result, announced its intention to capture and prosecute those responsible, which had the immediate effect that the FBI's ongoing intercepts were no longer for the "primary" purpose of foreign intelligence gathering – the "primary" purpose was now clearly prosecution. And as a result, in the middle of a terrorist crisis, the FBI turned *off* its listening devices for fear of violating the prohibition against using intelligence gathering techniques in a situation where intelligence gathering was not the primary purpose. It is difficult to conceive of a more wrong-headed course of

77. These intelligence-gathering mechanisms typically involved the application for a warrant to the Foreign Intelligence Surveillance Court (FISC), a court created by the Foreign Intelligence Surveillance Act (FISA). The FISC, which hears applications *ex parte* and often *in camera*, authorizes foreign intelligence information gathering acts (e.g. wiretaps or subpoenas for information).

78. *E.g.*, U.S. v. Truong, 629 F.2d 908 (4th Cir. 1980).

79. *See* Procedures for Contacts Between the FBI and the Criminal Division Concerning Foreign Intelligence and Foreign Counterintelligence Investigations, July 19, 1995, *cited in* In re: Sealed Case, 310 F.3d at 727-28; *see also* Final Report of the Attorney General's Review Team on the Handling of the Los Alamos National Laboratory Investigation, ch. 20, at 721-34, May 2000, *cited in Sealed Case*, 310 F.3d at 728 (describing effects of wall); "Primary Purpose" and the Sharing of Information Among the FBI, OIPR, and the Criminal Division, *available at* http://www.usdoj.gov/ag/readingroom/bellows20.pdf (undated memorandum describing effect of July Guidelines).

80. *Sealed Case*, 310 F.3d at 743.

81. Victoria Toensing, *Justice is Blind, Not Deaf*, WALL ST. J., Nov. 22, 2002, at A12.

conduct, yet the FBI, rightly, felt that it was legally obliged to act as it did.

Nor is this the only instance in which the artificial "wall" has deterred vital information sharing between law enforcement and intelligence communities. Who can forget the testimony of FBI agent Coleen Rowley, who pointed to these very limitations as part of the reason the FBI was not able to "connect the dots" before September 11th.[82] Instead, the culture against information sharing was so deeply ingrained that during the criminal prosecutions for the first 1993 World Trade Center bombing, the Department of Justice actually raised the height of the artificial wall. Imposing requirements that went "beyond what is legally required," the Department instructed its FBI agents to "clearly separate" ongoing counterintelligence investigations from the criminal prosecution.[83] There is even some possibility that this wall may have been the contributing factor to our failure to prevent the attacks of September 11th.[84]

Sections 202, and 218 tear down this wall, and empower federal agencies to share information on terrorist activity. This is an important, significant, positive development. One of the principle criticisms made in virtually every review of our pre-September 11th actions is that we failed to "connect the dots." Indeed, as the Congressional review panel noted: "Within the Intelligence Community, agencies did not share relevant counter-terrorism information, prior to September 11th. This breakdown in communications was the result of a number of factors, including differences in agencies' missions, legal authorities and cultures."[85]

---

82. *See* Testimony of Coleen Rowley Before the United States Senate Committee on the Judiciary, June 6, 2002, *available at* http://judiciary.senate.ogv/testimony.cfm?id=279 &wit_id=628.

83. *See* Memorandum from Jaime S. Gorelick, Deputy Attorney General, *Instructions on Separation of Certain Foreign Counterintelligence and Criminal Investigations* (1995).

84. *See* Testimony of Attorney General John Ashcroft before the National Commission on Terrorist Attacks Upon the United States (Apr. 13, 2004). The Attorney General quotes one frustrated FBI agent who wrote:

> Whatever has happened to this – someday someone will die – and wall or not – the public will not understand why we were not more effective and throwing every resource we had at certain 'problems.' Let's hope the National Security Law Unit [of the FBI] will stand behind their decision then, especially since the biggest threat to us, UBL [Usama Bin Laden], is getting the most protection.

Id.

85. *Report of the Joint Inquiry Into the Terrorist Attacks of September 11, 2001*, House Permanent Select Committee on Intelligence and Senate Select Committee on Intelligence, 107th Cong., 2nd Sess., S. Rep. No. 107–351 and H. Rep. No. 107–792, Dec. 2002, Finding 9, at xvii, *available at* http://www.fas.org/irp/congress/2002_rpt/911rept.pdf; *see also id.* at

In short, the Patriot Act changes adopt as a general principle the rule that *any information lawfully gathered during a foreign or domestic counter-intelligence investigation or lawfully gathered during a domestic law enforcement investigation should be capable of being shared with other federal agencies.* The artificial limitations we have imposed on such information sharing are a relic of a bygone era and, in light of the changed nature of the terrorist threat, are of substantially diminished value today.

We have already had at least one test case demonstrating the potential utility of enhanced information sharing between intelligence and law enforcement organizations: the indictment of Sami Al-Arian for providing material support to several Palestinian terrorist organizations.[86] The case, of course, has yet to be tried and Mr. Al-Arian is by law innocent until proven guilty. Thus, the truth of the government's assertions about him remains unproven and has yet to be tested.

But let us consider a hypothetical case and indulge in the assumption that the allegations are true. Let us imagine that, six months from now, the trial is over. If the allegations made in the indictment are substantiated, what will we have learned? Most pressingly, we will have learned that the charges against Mr. Al-Arian were delayed for at least 5 years by self-imposed legal obstacles barring the sharing of information between foreign counter-intelligence and domestic law enforcement organizations.

The government's case against Mr. Al-Arian is apparently based upon foreign counter-intelligence wiretap intercepts that date back as far as 1993. According to the information in those wiretaps, Mr. Al-Arian is charged with having knowingly provided financing to a terrorist organization with the awareness that the funds he provided would be used to commit terrorist acts. And that information has been in the possession of our intelligence organizations for at least the past 7 years.

It was not until the passage of the Patriot Act, and the ruling of the Foreign Intelligence Surveillance Court of Review in November 2002, that the intelligence community felt it was lawfully in a

---

Finding 1, at xv (concluding that both Intelligence Community and FBI were not well organized to address domestic terrorism threat).

86. *See* U.S. v. Al Arian, Indictment (M.D. Fla., *available at* http://news.findlaw.com/hdocs/docs/alarian/usalarian0203ind.pdf; *see also* U.S. v. Al-Arian, 280 F. Supp. 2d 1345 (M.D. Fla. 2003); United States v. Al-Arian, 267 F. Supp.2d 1258 (M.D. Fla. 2003); Matter of Search of Office Suites for World and Islamic Studies Enterprises, 925 F. Supp. 738 (M.D. Fla. 1996).

position to provide that information to law enforcement officials at the DOJ and the FBI. Only those changes enabled the government to bring the charges pending against Mr. Al-Arian.

If this is true, then we have made a wise change in policy. No one, not even Mr. Al-Arian, has publicly argued that the original foreign intelligence scrutiny of Mr. Al-Arian was unlawful or unwarranted. If it really is the case that one branch of our government lawfully had in its possession information about the criminal activity of a foreign national on American soil and that that branch was (or believed it was) obliged by law not to disclose that information to other branches of the government, then that fact alone will make some of the changes wrought by the Patriot Act worthwhile. To the extent that the law removed longstanding statutory barriers to bringing information gathered in national security investigations into federal criminal courts, it is to be welcomed.[87]

Nor can it be convincingly argued that the changes we have undertaken are violative of the Constitution. To the contrary, as the Court of Review recently made clear, the perverse wall between intelligence and law enforcement was not constitutionally required, and thus, that removing was constitutionally permissible. As the court said, the change wrought by the Patriot Act "is a reasonable response based on a balance of the legitimate need of the government for foreign intelligence information to protect against national security threats with the protected rights of citizens."[88] This is so because, as the court recognized (and as this paper argues) there is a difference in the nature of "ordinary" criminal prosecution and that directed at foreign intelligence or terrorism crimes: "The main purpose of ordinary criminal law is twofold: to punish the wrongdoer and to deter other persons in society from embarking on the same course. The government's concern with respect to foreign intelligence crimes, on the other hand, is overwhelmingly to stop or frustrate the immediate criminal activity."[89]

This is not to say that we disregard the past. We cannot, and should not, ignore recent unfortunate examples of government excess: For example, the abuses of the FBI's COINTELPRO (counterintelligence program) in the 1960's and 1970's, when investiga-

87. Al-Arian's case is not unique. The arrest of a suspected terrorist cell in Lackawanna, New York was also aided by the sharing of information. *See* ROSEN, *supra* note 29, at 142.

88. *Sealed Case*, 310 F.3d at 742.

89. *Id.* at 744.

tive authority was used to conduct surveillance of anti-war activists and civil rights groups.[90] Similarly, as the Church Committee investigation disclosed, our intelligence agencies have in several instances acted beyond the bounds of the law.[91] The limitations that restrained our activity prior to September 11th grew out of those revelations and were an appropriate, understandable reaction to excess.

But we can no longer afford to hamstring our counter-terrorism efforts in that way. The right answer is oversight and control, not complete rejection of enhanced government capacity to combat terror. And, these sections provide that oversight – no FISA warrant issues without the approval of a neutral federal judge who reviews each application. Though the forum has changed, and the subject matter of the investigation has been expanded, those changes appear sensible in light of the need to maintain the confidentiality of national security information used in securing the requisite authority. It is therefore no surprise that, as adumbrated above, the courts have already made clear "that FISA as amended is constitutional because the surveillances it authorizes are reasonable."[92]

Nor are the courts the only oversight mechanism in place. Portions of Section 202 and all of Section 218 are temporary. The increased information sharing authority granted to the government will "sunset" in December 2005. Thus, the oversight function of Congress is doubly important. It acts as a direct restraint on executive abuse through review. It will also be used to assess the utility of the changes that have occurred. Based upon our limited experience thus far, it seems that the advantages gained are substantially greater than the potential dangers posed by changes in the investigative authority granted the executive branch – but Congress will make assessment on a full record when it reconsiders these portions of the Patriot Act next year. In doing so, it would be wise to remember the past – and the problems that it identified as requiring change when it initially adopted the Patriot Act.

---

90. *See, e.g.*, Hobson v. Wilson, 737 F.3d 1 (D.C. Cir. 1984).

91. *See* Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, S. Rep. No. 94-755, 94th Cong. 2d Sess. (1976).

92. *Sealed Case*, 310 F.3d at 746.

B. Increased Investigative Authority and Business Records

Perhaps no provision of the Patriot Act has excited greater controversy than has Section 215, the so-called "angry librarians" provision. The section allows the FISA court in a foreign intelligence investigation to issue an order directing the recipient to produce tangible things. The revised statutory authority is not wholly new. FISA has had authority for securing some forms of business records since its inception. The new statutes modifies FISA's original business-records authority in a two important respects:

> • First, it "expands the types of entities that can be compelled to disclose information. Under the old provision, the FISA court could order the production of records only from 'a common carrier, public accommodation facility, physical storage facility or vehicle rental facility.'" The new provision contains no such restrictions.
>
> • Second, the new law "expanded the types of items that can be requested. Under the old authority, the FBI could only seek 'records.' Now, the FBI can seek 'any tangible things (including books, records, papers, documents, and other items).'"[93]

Thus, the modifications made by Section 215 do not explicitly authorizing the production of library records, but by its terms it authorizes orders to require the production of virtually any business record – and that might include library records, though it would include as well, airline manifests, international banking transaction records, and purchase records of all sorts. Critics of the Patriot Act have decried this provision,[94] but that criticism in this instance reflects an error of the first kind identified – mistaking the potential for abuse with the reality.

---

93. Department of Justice, *The USA Patriot Act: Myth vs. Reality* 16 (2003).

94. "Many [people] are unaware that their library habits could become the target of government surveillance. In a free society, such monitoring is odious and unnecessary . . . The secrecy that surrounds section 215 leads us to a society where the 'thought police' can target us for what we choose to read or what Websites we visit." *See* ACLU, *ACLU of New Mexico Seeks to Protect Individual Privacy*, TORCH, ACLU-New Mexico, July-Aug. 2003. The false image created is, as one writer has characterized it, of "white-haired and apple-cheeked [librarians] resisting as best they can the terrible forces of McCarthyism, evangelical Christian book-burning, middle-class hypocrisy, and Big Brother government." Joseph Bottum, *The Library Lie*, THE WKLY. STANDARD, Jan. 26, 2004, at 7. While politically appealing, the image simply does not match reality.

First, and most saliently, Section 215 mirrors, in the intelligence-gathering context, the scope of authority that already exists in traditional law enforcement investigations. Obtaining business records is a long-standing law enforcement tactic. Ordinary grand juries for years have issued subpoenas to all manner of businesses, including libraries and bookstores, for records relevant to criminal inquiries. For example, in the 1997 Gianni Versace murder case, a Florida grand jury subpoenaed records from public libraries in Miami Beach and in the 1990 Zodiac gunman investigation, a New York grand jury subpoenaed records from a public library in Manhattan. Investigators believed that the gunman was inspired by a Scottish occult poet, and wanted to learn who had checked out his books.[95] In the Unabomber investigation, law enforcement officials sought the records of various libraries, hoping to identify the Unabomber as a former student with particular reading interests.[96]

Section 215 merely authorizes the FISA court to issue similar orders in national-security investigations. It contains a number of safeguards that protect civil liberties. First, Section 215 requires FBI agents to get a court order. Agents cannot use this authority unilaterally to compel any entity to turn over its records. FISA orders are *unlike* grand jury subpoenas, which are requested without court supervision and are only subject to challenge *after* they have been issued.

Second, Section 215 has a narrow scope. It can only be used (1) "to obtain foreign intelligence information not concerning a United States person"; or (2) "to protect against international terrorism or clandestine intelligence activities." It cannot be used to investigate ordinary crimes, or even domestic terrorism. Thus, the scope is substantially narrower than the scope of traditional law enforcement investigations – for in those investigations, the grand jury may see the production of any business records unless the

95. *See Patriot Acting Out*, WALL ST. J., Jan. 22, 2004. The original source for this information is a Department of Justice publication, *supra* note 93, at 14.

96. *See* James Richardson and Cynthia Hubert, *Unabomber used library at UC Davis?*, SACRAMENTO BEE, Apr. 10, 1996, *available at* http://www.unabombertrial.com/archive/1996/041096-1.html (reporting that UC Davis library provided a book to the FBI with markings relating to the Unabomber's manifesto); *cf.* Patrick Hoge, *Rural acquaintances say Kaczynski attracted little notice*, Sacramento Bee, Apr. 5, 1996, *available at* http://www.unabombertrial.com/archive/1996/040596-2.html (reporting on Kaczynski's reading habits at library in Montana). Some courts have interpreted their State constitutions to provide a First Amendment protection that does not exist in Federal law. *See, e.g.*, Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044 (Colo. 2002).

subpoena recipient can demonstrate that "there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation,"[97] without the necessity of showing a connection to foreign intelligence activity or without the limitation that prevents subjecting United States persons to scrutiny in investigations of foreign intelligence activity – the grand jury may inquire into potential violations of *any* federal crime.[98]

Critics make two particular criticisms of this provision – that the judicial review it provides for is a chimera, and that the provisions of Section 215 imposing secrecy on the recipients of subpoenas issued pursuant to the section imposes a "gag rule" that prevents oversight of the use of the section's authority. Neither criticism, however, withstands close scrutiny.[99]

Section 215 provides for judicial review of the application for a subpoena for business records. The language provides, however, that upon application, the court "shall" issue the requested subpoena. From the use of the word "shall," critics infer that the obligation to issue the requested subpoena is mandatory and, thus, that the issuing court has no discretion to reject an application. Of course, if this were true (which, as discussed *infra*, it is not), then the absence of any judicial ability to reject an application would reduce the extent of judicial oversight.

But critics who make this argument (even if it were the case) miss the second order effects of judicial review. It imposes obligations of veracity on those seeking the subpoenas and to premise an objection on the lack of judicial review is to presuppose the mendacity of the subpoena affiants. It is also to presuppose the absence of any internal, administrative mechanisms in order to check potential misuse of the subpoena authority. And, most no-

97. U.S. v. R. Enters., Inc., 498 U.S. 292, 301 (1991).

98. A "United States person" is defined in Exec. Order 12333, pt. 3.4, as "a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States. . . ." Exec. Order No. 12333, pt. 3.4, 1981 WL 76054 (Dec. 4, 1981).

99. In the S.1709 (108th Cong.), the Security and Freedom Ensured Act of 2003 (called the "SAFE" Act by it's sponsors), it has been proposed to require a showing of "specific and articulable facts" before a § 215 order may be issued. *See* S.1709 (108th Cong.) § 4(a)(2). That showing would impose a greater obligation on law enforcement in an intelligence investigation than under the simple "relevance" standard that applies to federal grand juries investigating ordinary criminal offenses. In part for this reason, the Administration has threatened to veto the SAFE Act if it is passed. *See* Letter from Atty. General Ashcroft to Sen. Orin Hatch (Jan. 28, 2004).

tably, it presupposes that the obligation to swear an oath of truthfulness, with attendant perjury penalties for falsity, has no deterrent effect on the misuse of authorities granted.[100]

But even more significantly, this criticism misreads the statute, which, while saying that the subpoena "shall" issue, also says that it shall issue as sought *or* "as modified." The reviewing judge thus, explicitly, has authority to alter the scope and nature of the documents being sought – a power that cannot be exercised in the absence of substantive review of the subpoena request. Thus, the suggestion that the provisions of Section 215 preclude judicial review is simply mistaken – to the contrary, it authorizes judicial review and modification of the subpoena request which occurs before the subpoena is issued – a substantial improvement over the situation in traditional grand jury investigations where the subpoena is issued without judicial intervention, and the review comes, at the end, only if the subpoena is challenged.

Nor is judicial oversight the only mechanism by which the use of Section 215 authority is monitored. The section expressly commands that the Attorney General "fully inform" Congress of how the section is being implemented. And on October 17, 2002, the House Judiciary Committee, after reviewing the Attorney General's first report, indicated that it was satisfied with the Department's use of section 215: "The Committee's review of classified information related to FISA orders for tangible records, such as library records, has not given rise to any concern that the authority is being misused or abused."[101]

The second criticism – that Section 215 imposes an unwarranted gag rule – is equally unpersuasive. Section 215 does prohibit recipients of subpoenas from disclosing that fact – a precaution that is necessary to avoid prematurely disclosing to the subjects of a terrorism investigation that they are subject to government scrutiny. That prohibition might be independently justified,

---

100. For a similar point, *see* Daniel Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1124-28 (2002) (highlighting the significance of judicial oversight and warrant requirements in maintaining an "architecture of power" to protect privacy). Warrants raise the "standard of care of law enforcement officials by forcing them to document their requests for authorization" and the "requirement of prior approval prevents government officials from dreaming up post-hoc rationalizations." *Id.* at 1126-27. This provides an institutional/procedural check on abuse even if we assume that magistrates routinely defer to police and prosecutors.

101. *See* Statement of F. James Sensenbrenner, Jr. Chmn. House Jud. Comm., Oct. 17, 2002, *available at* http://www.house.gov/judiciary/news101702.htm.

given the grave nature of the potential threats being averted (that is, given the nature of the Type II errors involved).

But it need not be – for, again, the secrecy provisions of Section 215 merely extend existing rules in traditional law enforcement grand juries to the more sensitive intelligence arena. In the grand jury context, it is common for third party records custodians to be prohibited from disclosing the existence of the document request. Banks, for example, may be obliged to conceal requests made to them.[102] And it is clear, beyond peradventure, that these grand jury secrecy obligations are constitutional. For example, when the nanny of Joan Benet-Ramsey was called to testify before a state grand jury, state law prohibited her from disclosing the substance of her testimony. When she challenged that law (on the ground that it infringed her freedom of speech), her challenge was rejected by the courts.[103]

In short, critics of Section 215 make a very difficult and, in the end, unpersuasive argument. They offer the view, in effect, that traditional law enforcement powers that have been used in grand juries for years to investigate common law crimes and federal criminal offenses ought not to be used with equal authority to investigate potential terrorist threats. To many, that argument seems to precisely reverse the evaluation – if anything, the powers used to investigate terrorism, espionage and threats to national security ought to be greater than those used to investigate mere criminal behavior.[104] This is not, of course, to denigrate the significance and seriousness of many federal and state crimes – but it is to recognize that however grave those crimes are, they do not pose the same risk to the foundations of American society or to the security of large numbers of citizens as the risks posed by potential terrorist acts.

Critics of Section 215 do, however, have one strong argument against renewal of the Section 215 authority (which also sunsets

---

102. 12 U.S.C. § 3604(c).

103. *Hoffmann-Pugh v. Keenan*, 338 F.3d 1136 (10th Cir. 2003); *see also Hoffman-Pugh v. Ramsey*, 312 F.3d 1222 (11th Cir. 2002) (rejecting libel suit filed by nanny against the Ramsey family).

104. This view is not an idiosyncratic one. At the time the Patriot Act was passed, Senator Biden (D-DE) argued that "the FBI could get a wiretap to investigate the mafia, but they could not get one to investigate terrorists. To put it bluntly, that was crazy! What's good for the mob should be good for terrorists." Cong. Rec. at S11048, Oct. 25, 2001, *available at* http://www.lifeandliberty.gov/subs/support/senbiden102501_1.pdf, *quoted in* Barbara Comstock, *Prez Calls Dems Patriot Games Bluff*, NAT'L REV. ONLINE, Jan. 21, 2004, *available at* http://www.nationalreview.com/comment/comstock200401211300.asp.

in December 2005) – that the authority granted may be unnecessary. Facing wide public criticism of the provisions of the section 215, the Attorney General has disclosed that, at least as of September 2003, the provision had not been used to secure any records.[105] It would seem that, since almost all terrorist acts are also federal crimes, existing grand jury subpoena authority has been sufficient to allow the government to secure all of the information it has needed in the months since September 11th. But it is important to recognize that this is a question of *utility*, not a question of *abuse*. And we know that the September 11th terrorists did use internet connections at libraries to communicate, well prior to the existence of any predication that they had committed a crime.[106] Thus, the potential utility of the section exists. As a consequence, when Section 215 comes up for review, Congress will need to carefully evaluate whether or not continuation of that authority is necessary.

But that review must be grounded in a solid understanding of what Section 215 actually authorizes. It should not be swayed by the public mythology that surrounds this provision. That myth has led to the rather absurd result that some librarians are destroying their borrowing records in order to prevent them from becoming available to the federal government.[107] In other words, those charged in our society with protecting and maintaining knowledge and information are destroying it. The interest in protecting civil liberties must be high – but not so high that we unnecessarily and unwisely lapse into hysteria.[108]

---

105. *See* Memorandum for Director Robert S. Muller, Sept. 18, 2003, *available at* http://www.cdt.org/security/usapatriot/030918doj.shtml.

106. *See, e.g.*, Farhad Manjoo, *Terrorists Leave Paperless Trail*, WIRED NEWS, Sept. 20, 2001, *available at* http://www.wired.com/news/politics/0,1283,46991,00.html.

107. *See, e.g.*, Sen. Russ Feingold, Speech on the Libraries, Bookseller and Personal Records Privacy Act, Mar. 7, 2003, *available at* http://feingold.senate.gov/speeches/03/07/2003811915.html (reporting such events); ACLU, *ACLU of Florida Urges Libraries to Warn Patrons of Government's New Domestic Spying Powers Under the USA Patriot Act*, July 30, 2003, *available at* http://www.aclufl.org/body_section215release.html (same).

108. As former Attorney General Meese has noted, the position adopted by librarians is particularly odd when contrasted with their long-standing opposition to federal provisions restricting children's on-line access to pornography. It is at least a little jarring that librarians see it as their duty to protect the access of minors to pornography while denying the government access to information of national security importance. *See NBC News: Today* (NBC television broadcast, Sept. 30, 2003) (transcript available at 2003 WL 55607752). The American Library Association has also declined to condemn Fidel Castro's jailing of librarians. *See* Nat Hentoff, *Carrying Fidel's Water*, WASH. TIMES, Jan. 26, 2004, at A19.

C. Searches and Seizures – Delayed Notification

Another section of the Patriot Act that has engendered great criticism is Section 213, which authorizes the issuance of delayed notification search warrants – the so-called "sneak and peek" warrants. Traditionally, when the courts have issued search warrants authorizing the government's forcible entry into a citizen's home or office, they have required that the searching officers provide contemporaneous notification of the search to the individual whose home or office has been entered.[109] Prior to September 11th, some courts permitted limited delays in notification to the owner, when immediate notification would hinder the ongoing investigation. Section 213 codifies that common law tradition, and extends it to terrorism investigations. Critics see this extension as an unwarranted expansion of authority – but here too, the fears of abuse seem to outstrip reality.[110]

Delayed notification warrants are a long-existing, crime-fighting tool upheld by courts nationwide for decades in organized crime, drug cases and child pornography. For example, Mafia Don Nicky Scarfo maintained the records of his various criminal activities on a personal computer, protected by a highly sophisticated encryption technology. Law enforcement knew where the information was – and thus had ample probable cause to seize the computer. But the seizure would have been useless without a way of breaking the encryption. So, on a delayed notification warrant, the FBI surreptitiously placed a keystroke logger on Scarfo's computer – the logger recorded Scarfo's password and, with the password, the FBI was able to examine all of Scarfo's records of his various drug deals and murders.[111] It would, of course, have been fruitless for the FBI to have secured a warrant to enter Scarfo's

109. The requirement has a long-standing provenance in common law. As the King's Bench court said in 1603: "In all cases where the King is a party, the sheriff . . . may break the party's house, either to arrest him, or to do execution of the King's process, if otherwise he cannot enter. But before he breaks it, he ought to signify the cause of his coming, and to make request to open the doors." Semanyne's Case, 77 Eng. Rep. 194 (K.B. 1603).

110. Some, for example, implicitly argue that the Section 213 authority is novel: "The Patriot Act allows the use of so called 'sneak and peek' warrants without informing the occupants if a judge decides that giving notice would hurt the government's investigation," ROSEN, *supra* note 29, at 137. As the text makes clear, the Patriot Act neither creates a new procedure nor permits the permanent elimination of a notification requirement.

111. U.S. v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001).

home and place a logger on his computer if, at the same time, it had been obliged to notify Scarfo that it had done so.[112]

This common law use of delayed notification has been approved by the courts. Over 20 years ago, the Supreme Court held that the Fourth Amendment does not require law enforcement to give immediate notice of the execution of a search warrant. The Court emphasized "that covert entries are constitutional in some circumstances, at least if they are made pursuant to a warrant." In fact, the Court stated that an argument to the contrary was "frivolous."[113] In an earlier case – the seminal case defining the scope of privacy in contemporary America – the Court said, "officers need not announce their purpose before conducting an otherwise [duly] authorized search if such an announcement would provoke the escape of the suspect or the destruction of critical evidence." [114]

Section 213 of the Patriot Act thus attempts to codify the common law authority that law enforcement had already had for decades. "Because of differences between jurisdictions, the law was a mix of inconsistent standards that varied across the country. This lack of uniformity hindered complex terrorism cases. Section 213 resolved the problem by establishing a uniform statutory standard."[115] Now, under section 213, courts can delay notice if there is "reasonable cause" to believe that immediate notification may have a specified adverse result. The "reasonable cause" standard is consistent with pre-PATRIOT Act case law for delayed notice of warrants.[116] And the law goes further, defining "reasonable cause" for the issuance of a court order narrowly. Courts are, under section 213, authorized to delay notice only when immediate notification may result in death or physical harm to an individual, flight from prosecution, evidence tampering, witness intimidation, or otherwise seriously jeopardize an investigation.[117]

---

112. The same, of course, is true of any surreptitious use of listening devices. It would have done little good for the FBI to secure a warrant to enter John Gotti's eating club in Brooklyn to place a recording device in the facility if it had been obliged, at the same time, to politely let Gotti know that he needed to speak clearly into the chandelier, as that was where the bug had been placed.

113. Dalia v. U.S., 441 U.S. 238 (1979).

114. Katz v. U.S., 389 U.S. 347 (1967).

115. Dept. of Justice, *supra* note 93, at 11.

116. *See, e.g.,* U.S. v. Villegas, 899 F.2d 1324, 1337 (2d Cir. 1990) (government must show "good reason" for delayed notice of warrants).

117. Section 213 cross-references and adopts the standards used to authorize delayed notification of a wiretap or other electronic interception of communication. *See* 18 U.S.C. § 2705(a)(2). Some critics say that this final catch-all phrase is too broad and provides for too much leeway for Executive action. *See* SAFE Act, S.1709 (108th Cong.) § 3(a)(1)(A)

In short, section 213 is really no change at all – it merely clarifies that a single uniform standard applies and that terrorist offenses are included. Nor does Section 213 promise great abuse. Here, as in the past under common law, the officer seeking authority for delayed entry must get authorization for that action from a federal judge or magistrate – under the exact same standards and procedures as they would need to do so to get a warrant to enter a building in the first place. And the law makes clear that in all cases law enforcement must ultimately give notice that property has been searched or seized – the only difference from a traditional search warrant is the temporary delay in providing notification. Here, too, then the presence of oversight rules seems strong – certainly strong enough to prevent against the abuse that some critics fear.[118]

Nor can it be doubted that the delayed notification have performed a useful function and are a critical aspect of the strategy of prevention – detecting and incapacitating terrorists *before* they are able to strike. One example of the use of delayed notification involves the indictment of Dr. Rafil Dhafir. A delayed notification warrant allowed the surreptitious search of an airmail envelope containing records of overseas bank accounts used to ship over $4 million to Iraq. Because Dhafir did not know of the search, he was unable to flee and he did not move the funds before they were seized.[119] In another instance, the Department described a hypothetical (based upon an actual case) in which the FBI secured access to the hard drive of terrorists who had sent their computer for

---

(proposing to eliminate catch-all clause and "intimidation of potential witnesses" as grounds for delayed notification). In the main, this concern seems overly cautious – one can imagine few circumstances in which an investigation would be "seriously jeopardized" that would not also satisfy one of the more specific listings of potential adverse consequences that seem, undoubtedly, to be appropriate grounds for delay. But more problematically, in making that argument critics must accept, implicitly, the converse proposition – that there are circumstances in which an Article III judge would find that an investigation would be seriously jeopardized but in which they would not accept a delay in notification. In other words, they value the process of notification more highly than the substance of an impaired investigation – a result that seems to reverse the more reasonable evaluation of the comparative values, especially when the result is validated by an independent Federal judge.

118. The Department of Justice has reported to Congress that the most common period of delay has been 7 days. Delays as short as 1 day or as long as 90 have been authorized. On occasion, courts have permitted delays for an unspecified period of time lasting until an indictment was unsealed. *See* Letter, Janice E. Brown, Act'g Asst. Atty. Gen. to Hon. James Sensenbrener, Chrmn. House Jud. Comm., Attachment at 10 (May 12, 2003).

119. *See* Letter, William E. Moscella, Asst. Atty. Gen. to Hon. Dennis Hastert, Speaker, at 3 (July 25, 2003); *see also* AP, *Four Indicted for Sending Funds to Iraq*, HOUS. CHRON., Feb. 26, 2003, *available at* http://www.chron.com/cs/CDA/printstory.hts/special/iraq/1796320.

repair. In still another, they planted a bug in a terrorists' safe house.[120]

Finally, opposition to Section 213 seems to misunderstand the true nature of the Type I error involved. The purpose of the notice requirement is two-fold: 1) In typical searches it allows a contemporaneous objection. The individual may say, in effect, "you've got the wrong house;" 2) Following notification it also allows for non-contemporaneous objections to be heard in court – so that overzealous execution of the warrant, or a search beyond the scope authorized may be challenged before a judge.

But in the context of a surreptitious entry and delayed notification, the first of those purposes can have no force. Except by accident law enforcement or intelligence agents will not conduct a delayed notice entry in a manner that affords contemporaneous notification – to do so would frustrate the precise purpose of the delayed notification. So the *only* way to effectuate the first of these two purposes is to prohibit delayed notification entry altogether, a rule that would have very significant costs. And it is equally clear that the second purpose – allowing subsequent challenge in court – is served so long as the law requires (as Section 213 does) eventual notification in all circumstances. The only real argument that critics can make is that Section 213 imposes costs by virtue of the time for which the notification is delayed – a true cost but a comparatively minor one when balanced against the substantial benefits that the process of delayed notification allows.

The evident utility of the potential uses of Section 213, the provision for subsequent review in court, and the absolute absence of any evidence of abuse of this power, suggest that several proposed repeals under Congressional consideration are unwise.[121] At worst, they would completely eliminate a long-standing investigative tool for all crimes – both terrorist crimes, and traditional common law crimes. At best, the rejection of Section 213 would reinstitute a dichotomy between traditional crimes and terrorist investigations – again, a mistaken one that oddly provides greater authority to investigate less threatening common law criminal acts.

---

120. *See* Moscella, *supra* note 119, at 4.

121. These proposals include, *e.g.*, S. 1709 (108th Cong.) (introduced by Sen. Craig (R-ID) and Sen. Durbin (D-IL)) (proposing substantial curtailment of the Patriot Act); S. 1552 (108th Cong.) (introduced by Sen. Murkowski (R-AK)) (same); H. Amdt. 292 to H.R. 2799 (108th Cong.) (introduced by Rep. Otter (R.-ID)) (proposing to prohibit funds to carry out Section 213).

This reaction to Section 213 does, however, highlight one significant aspect of the changing nature of the public debate concerning civil liberties – the greater awareness of issues relating to governmental authority that the events of September 11th have engendered in the general public. The common law authority to delay notification has existed for more than 20 years. It took the events of September 11th to make the public generally aware of that authority. And that is a good thing – for though some might disagree on whether such authority is necessary, few can disagree that an intelligent and thoughtful debate about the utility of such authority amongst the public and its elected representatives benefits everybody.

D. Threats To Protected First Amendment Advocacy

In at least two ways, aspects of the Executive response to terror have directly raised the specter of a potential threat to core First Amendment advocacy – opposition, for example, to the Administration's policy regarding Iraq, or globalization of the economy. Unlike the two aspects of the Patriot Act already discussed (where the costs of Type II errors are high, and the relative risk of Type I errors minimal), here the costs of a Type I error are higher. The fundamental right to openly criticize the government is a broad public right, held by all in common. As such, we should be especially careful before allowing new policies to trench upon that right.

1. FBI Revised Investigative Guidelines

Consider, first, certain new FBI investigative guidelines.[122] These new guidelines, announced by the Attorney General in May 2002,[123] authorize FBI agents to open up anti-terror investigations

122. These guidelines were, as the text makes clear, of purely executive character, reversing earlier executive orders originally promulgated in the 1970's. The most recent reissuance prior to 2001 was in November of 1995. *See* Advice to FBI Regarding Domestic Security/Terrorism Investigations and Preliminary Inquires (Nov. 21, 1995). As executive orders, they have no formal relationship to the Patriot Act. Yet, concern over the "FBI invading mosques" is one of the perpetual criticisms of the Patriot Act – reflecting the public's broader conception of the Act than the reality of its parameters. As such, it seems appropriate to address the issue in this paper which deals with the broad context of civil liberty and the necessities of anti-terrorism investigations.

123. *See* The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations, May 2002, *available at* http://www.usdoj.gov/olp/generalcrimes2.pdf.

whenever information warrants. They have stirred controversy, at least in part, because the guidelines now allow FBI agents conducting such investigations to do so in any public forum – in effect, allowing agents to attend anti-war rallies or prayer at mosques in order to discern whether the line between permissible First Amendment advocacy and impermissible advocacy of specific violent acts has been crossed.

American policy has a historic, long-standing tolerance for dissent – even dissent that advocates change in the government.[124] As Justice Oliver Wendell Holmes wrote: "The best test of truth is the power of the thought to get itself accepted in the competition of the market . . . . [W]e should be eternally vigilant against attempts to check the expression of opinions that we loathe and believe to be fraught with death."[125] Thus, in 1969, the Supreme Court made clear that the law may not "forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing *imminent* lawless action."[126] In the light of terrorism threats, investigative practices to examine whether speech crosses that line from theoretical to imminent are perfectly reasonable and understandable – but if advanced too forcefully, they run the substantial risk of chilling protected speech.

There are, therefore, aspects of the FBI's guidelines that suggest the need for heightened sensitivity to the potential for an infringement on protected constitutional liberties. To be sure, the FBI guidelines raise no Fourth Amendment concerns, insofar as they authorize the FBI to collect publicly available information from public databases and/or public meetings – that information is not protected under the privacy doctrines that follow from *Katz*.

Nonetheless, the FBI guidelines do implicate potential threats to at least two fundamental liberty interests guaranteed by the Constitution. Most obviously, the Supreme Court has long recognized a freedom of political association and the threat to that free-

---

124. *But see* McConnell v. Fed. Election Comm'n, 124 S. Ct. 619 (2003) (allowing restrictions on political speech to combat appearance of corruption).

125. Abrams v. U.S., 250 U.S. 616, 630 (1919) (Holmes, J., dissenting).

126. Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (emphasis added); *see also* NAACP v. Clairborne Hardware, Co., 458 U.S. 886 (1982) (approving peaceful boycott). One caveat to this analysis is in order – in *Brandenburg*, and in earlier cases applying the "clear and present danger" doctrine, the actual threat of violence was "puny." *See Brandenburg*, 395 U.S. at 454 (Douglas, J. concurring). Whatever one thinks of the terrorist threat, there can be little argument that it is not as minimal as those "threats" previously addressed by the Court.

dom posed by requiring organizations to identify their members.[127] Second, many of the indicators that *might* be used to identify potential subjects of a terrorist investigation are also indicators that, in other circumstances, are potentially the products of protected First Amendment activity; in other words, though FBI investigative techniques are not intended to impinge upon free political speech or association, they may have the collateral effect of doing so.

Thus, there is a significant risk that a mal-administered system will impinge upon fundamental constitutional liberties. This does not mean that the risk of such impingement means abandonment of the program – especially not in light of the potentially disastrous consequences of another terrorist attack in the United States. However, fairly stringent steps are necessary to provide the requisite safeguards for minimizing inadvertent or abusive infringements of civil liberty in the first instance and correcting them as expeditiously as possible. Those steps would include some or all of the following:

> • The FBI's use of these new investigative guidelines should be subject to extensive, continuous Congressional oversight. This should include more than the mere reporting of raw data and numbers – at least as a spot check, Congress should examine individual, closed cases (if necessary using confidential procedures to maintain classified status) to assure itself that the investigative guidelines are not being misused. In other words, the database contemplated by the FBI guidelines should, under limited circumstances, be subject to congressional scrutiny;
>
> • Authorization for "criminal intelligence" investigations under the FBI's guidelines should, in all circumstances, be in writing such that the FBI's internal system creates an "audit trail" for the authorization of investigations with potential First Amendment implications. Only through detailed record keeping can the use and/or abuse of investigative authority be reviewed;

127. *See* NAACP v. Button, 371 U.S. 415 (1963) (defining freedom of association).

- The FBI's new guidelines generally authorize the use of all lawful investigative techniques for both "general crimes" investigations and "criminal intelligence" investigations. There should be a special hesitancy, however, in using the undisclosed participation of an undercover agent or cooperating private individual to examine the conduct of organizations that are exercising core First Amendment rights. When an organization is avowedly political in nature (giving that phrase the broadest definition reasonable) and has as its sole mission the advocacy of a viewpoint or belief, we should be especially leery of ascribing to that organization criminal intent, absent compelling evidence to that effect.

- There should, as well, be a hesitancy in visiting public places and events that are clearly intended to involve the exercise of core First Amendment rights, as the presence of official observers may chill expression. This is not to say that no such activity should ever be permitted – it is, however, to suggest the need for supervisory authorization and careful review before and after the steps are taken. Conversely, existing court consent decrees that expressly prohibit all such activity (as is currently the case in New York City)[128] should be revisited.

- No American should be the subject of a criminal investigation solely on the basis of his exercise of a Constitutionally protected right to dissent. An indication of threat sufficient to warrant investigation should always be based upon significant intelligence suggesting actual criminal or terrorist behavior.

Finally, although the FBI's guidelines authorize preliminary inquiries through the use of public information resources, many Americans fear that these inquiries will result in the creation of personalized dossiers on dissenters. As it appears now, there are no explicit provisions in the guidelines for the destruction of records from preliminary inquiries that produce no evidence sufficient to warrant a full-scale investigation. One possible amendment to the guidelines that would ameliorate many privacy con-

128. *See* Handschu v. Special Servs. Div., 605 F. Supp. 1384 (S.D.N.Y. 1985), *aff'd*, 787 F.2d 828 (2d Cir. 1985).

cerns would be an explicit provision providing for such destruction or, archiving with limited retrieval authority.

One other brief point should be made about privacy – one already made in the general discussion earlier. The FBI guidelines are not exclusively an impingement on privacy. Rather, they act by substituting one privacy intrusion (into certain public spheres) for other privacy intrusions (into more private spheres, perhaps through other investigative means). It may also substitute for increased random investigations or the invidious use of racial, national origin, or religious classifications. Here, one cannot make broad value judgments – as noted, each person weighs the utility of their own privacy by a different metric. But we should acknowledge that for some Americans, the price of a little less public privacy might not be too great if it resulted in a little more personal privacy.

2. *"Material Support" For Terrorism*

A second potential area in which the Patriot Act might be seen to impinge on First Amendment freedoms lies in the prohibition against providing material support to terrorist organizations.[129] Some organizations have humanitarian aspects to their work and say that their humanitarian efforts are distinct from the allegedly

129. Some raise yet another concern in the definition of "domestic" terrorism, added to the law by Section 802 of the Patriot Act. Some critics claim that this amendment "expands terrorism laws to include 'domestic terrorism' which could subject political organizations to surveillance, wiretapping, harassment, and criminal action for political advocacy." They also claim that it includes a "provision that might allow the actions of peaceful groups that dissent from government policy, such as Greenpeace, to be treated as 'domestic terrorism.'" *See* Stuart Taylor in *UnPATRIOTic*, NAT'L J., Aug. 4, 2003 (quoting ACLU fundraising letter); *see also* ACLU, *The USA Patriot Act and Government Actions that Threaten Our Civil Liberties* (undated). These fears are exacerbated by some government actions – there is, for example, a pending criminal charge against Greenpeace for boarding ships coming into American ports as a means of protest. *See* United States v. Greenpeace, Inc., Indictment (M.D. Fla No. 03-20577) (charging violation of 18 U.S.C. § 2279); *see also* U.S. Dept. of Justice, *Greenpeace Charged with Conspiracy to Unlawfully Board Cargo Vessel*, July 18, 2003, *available at* http://www.usdoj.gov/usao/fls/greenpeace.html. § 2279 proscribes, *inter alia*, "go[ing] on board any vessel . . . before her actual arrival" and was intended to prevent prostitutes and pimps from boarding arriving merchant ships.

These charges are, of course, independent of the Patriot Act, but they do lend credence to fears expressed about the potential to use the Patriot Act to suppress dissent. Insofar, however, as the Patriot Act itself is concerned, these fears are not well-grounded. The Patriot Act limits the definition of "domestic terrorism" in a way that protects political protest. Under § 802 of the Patriot Act, the definition of "domestic terrorism" is limited to conduct that (1) violates federal or state criminal law and (2) is dangerous to human life. Peaceful groups that dissent from government policy without breaking laws cannot be investigated.

terrorist acts of related organizations. They thus argue that it impinges on First Amendment freedoms of speech and association for supporters to be criminally prosecuted when all they are doing is providing material support to the humanitarian aspects of the organization. The Executive responds, not unreasonably, that money is fungible and that contributions to the humanitarian aspects of the organization are readily "passed through" to the terrorist arms of related organizations.[130] We thus face the difficult conundrum of distinguishing between conduct aimed to support legitimate political and humanitarian groups and conduct that is a mere subterfuge for supporting terrorist organizations.

It must, first, be acknowledged that much of the ambiguity in the statute pre-dates the Patriot Act itself. It was an earlier statute, the Anti-Terrorism and Effective Death Penalty Act of 1996, that gave the Secretary of the Treasury the authority to designate terrorist organizations, and made it a crime to provide material support to organizations so designated.[131] The Patriot Act, in Section 810, enhanced the criminal penalties and also, in Section 805, expanded the scope of the statute – making clear that it applied to those who provided expert assistance to terrorist organizations; applied to acts outside the United States; expanded the list of terrorism crimes for which it is illegal to provide material support; and clarified that material support includes all types of monetary instruments.

The question remains – what must the government prove the supporter knew in order for the supporter to violate the criminal prohibition? The statute states that "[w]hoever . . . knowingly provides material support to a foreign terrorist organization" is guilty of a crime.[132] Does it suffice to show that the supporter purposefully did the act which constitutes the offense – i.e. that he provided material support by donating money to the organization, or must government also show that the supporter knew of the organization's designation as a terrorist organization or of the unlawful activities that caused it to be so designated?[133]

---

130. Nor is the concern limited to the Executive Branch. The Senate Finance Committee has begun an investigation of certain charities, believing them to be fronts for Al-Qaeda fundraising. *See* Dan Eggen & John Mintz, *Muslim Groups' IRS Files Sought*, WASH. POST, Jan. 14, 2004, at A1.

131. *See* Anti-Terrorism and Effective Death Penalty Act of 1996, Pub. L. 104-31, 110 Stat. 1214, §§ 302, 303 (codified at 8 USC § 1189 and 18 USC § 2339B).

132. 18 USC § 2399B.

133. Humanitarian Law Project v. Dep't of Justice, 352 F.3d 382 (9th Cir. 2003).

Here, the Government's position – that it need not prove knowledge of the designation – goes too far and risks trenching on First Amendment freedoms of speech and association.[134] The requirement that a crime involve culpable purposeful intent has a solid historical grounding. As Justice Robert Jackson wrote:

> The contention that an injury can amount to a crime only when inflicted by intention is no provincial or transient notion. It is as universal and persistent in mature systems of law as belief in freedom of the human will and a consequent ability and duty of the normal individual to choose between good and evil. A relation between some mental element and punishment for a harmful act is almost as instinctive as the child's familiar exculpatory "But I didn't mean to," and has afforded the rational basis for a tardy and unfinished substitution of deterrence and reformation in place of retaliation and vengeance as the motivation for public prosecution. Unqualified acceptance of this doctrine by English common law was indicated by Blackstone's sweeping statement that to constitute any crime there must first be a "vicious will."[135]

Though the text of Section 2339B requires that the supporters have acted "knowingly" – a seeming protection from the imposition of unwarranted liability – if interpreted as the government suggests, that requirement would be but a parchment barrier to what is, in effect, the imposition of absolute liability. The government's interpretation would presume that all supporters are charged with knowing all of the intricate regulatory arcana that govern the designation by the Secretary of terrorist organizations – a presumption that generally applies (and perhaps misapplies) in the context of a closely regulated industry.[136] As a consequence, under the Government's interpretation, the only requirement imposed by requiring proof that one has acted "knowingly" is that the government must demonstrate that the defendant has purposefully

---

134. For a general discussion of the problem of overly broad criminal laws and the increased criminalization of otherwise innocent conduct, *see* Paul Rosenzweig, *The Over-Criminalization of Social and Economic Conduct*, LEGAL MEMORANDUM NO. 7 (The Heritage Foundation, Apr. 2003).

135. Morissette v. U.S., 342 U.S. 246, 250-51 (1952).

136. *E.g.*, U.S. v. Int'l Minerals & Chemical Corp., 402 U.S. 558, 565 (1971) ("[W]here . . . dangerous or deleterious materials are involved, the probability of regulation is so great that anyone who is aware that he is in possession of them or dealing with them must be presumed to be aware of the regulation.").

done the act constituting the offense – and in the context of a charitable donation that showing is trivial. Nobody donates by mistake or accident. As Justice Potter Stewart noted: "As a practical matter, therefore, they [would be] under a species of absolute liability for violation of the regulations despite the 'knowingly' requirement."[137]

What is particularly disturbing about the Government's argument is that it works in tandem with the statutory amendment authorizing significantly harsher penalties. Historically, when the courts first considered laws containing reduced intent requirements, the laws almost uniformly provided for very light penalties such as a fine or a short jail term, not imprisonment in a penitentiary.[138] As commentators noted, modest penalties are a logical complement to crimes that do not require specific intent.[139] Indeed, some courts questioned whether any imprisonment at all could be imposed in the absence of intent and culpability.[140] This historical view has, of course, been lost: laws with reduced *mens rea* requirements are often now felonies.[141] And even misdemeanor offenses can, through the stacking of sentences, result in substantial terms of incarceration.[142]

But this should not be the uniform case – especially where, as here, much innocent conduct, otherwise protected by the First Amendment, would be swept up in the broader definition. We should not lose sight of a fundamental truth: "If we use prison to achieve social goals regardless of the moral innocence of those we incarcerate, then imprisonment loses its moral opprobrium and our criminal law becomes morally arbitrary."[143] Or as the drafters of the Model Penal Code said:

---

137. *International Minerals & Chemical Corp.*, 402 U.S. at 569 (Stewart, J., dissenting).

138. *See* Staples v. U.S., 511 U.S. 600, 616 (1994) (citing, *e.g.*, Commonwealth v. Raymond, 97 Mass. 567 (1867) (fine up to $200 or 6 months in jail); Commonwealth v. Farren, 91 Mass. 489 (1864) (fine only); People v. Snowburger, 71 N.W. 497 (1897) (fine up to $500 or incarceration in county jail)).

139. *See* Francis B. Sayre, *Public Welfare Offenses*, 33 COLUM. L. REV. 55, 70 (1933); *see also Morissette*, 342 U.S. at 256 ("[P]enalties commonly are relatively small, and conviction does no grave damage to an offender's reputation").

140. *E.g.* People ex rel. Price v. Sheffield Farms-Slawson-Decker, Co., 121 N.E. 474, 477 (1918) (Cardozo, J.); *id.* at 478 (Crane, J., concurring) (imprisonment for crime that requires no *mens rea* stretches law of regulatory offenses beyond its limitations).

141. *E.g.*, U.S. v. Weitzenhoff, 35 F.3d 1275 (9th Cir. 1994) (felony violation of Clean Water Act; no knowledge of regulations necessary).

142. *E.g.*, U.S. v. Ming Hong, 242 F.3d 528 (4th Cir. 2001) (misdemeanor convictions stacked for 3 year sentence).

143. *Weitzenhoff*, 35 F.3d at 1293 (Kleinfeld, J., dissenting from denial of rehearing *en banc*).

> It has been argued, and the argument undoubtedly will be repeated, that strict liability is necessary for enforcement in a number of the areas where it obtains. But if practical enforcement precludes litigation of the culpability of alleged deviation from legal requirements, the enforcers cannot rightly demand the use of penal sanctions for the purpose. Crime does and should mean condemnation, and no court should have to pass that judgment unless it can declare that the defendant's act was culpable. This is too fundamental to be compromised.[144]

The broad statutory language, which does not make clear what intent must be proven has, fortunately, begun to be interpreted by the courts in a restrictive manner.[145] And that's a good thing – it demonstrates again that we can grant the government additional powers to combat terrorism while reasonably anticipating that the checking mechanisms in place will restrain too excessive a use of those powers.

E. Information Technology – The Next Challenge

Much of the foregoing discussion has focused on the primary fear that critics have – the fear of enhanced executive authority and the potential for abuse. As noted at the outset, however, there is a second aspect to the critique offered by opponents of new executive authority – concern that advances in information technology will unreasonably erode the privacy and anonymity to which American citizens are entitled. They fear, in effect, the creation of an "electronic dossier" on every American. While portions of the Patriot Act tangentially raise those fears,[146] the pre-

144. MODEL PENAL CODE § 2.05 and Comments at 282–83 (1985).

145. *Humanitarian Law Project*, 352 F.3d at 394-403. The Court also held that the terms "personnel" and "training" were impermissibly vague. *Id.* at 403-05. On remand, the district court likewise held that the phrase "expert advice" was impermissibly vague. *See* Humanitarian Law Project v. Ashcroft, 2004 WL 112760 (C.D. Cal. Jan. 22, 2004) (as reported in Eric Lichtblau, *Citing Free Speech, Judge Voids Part of Antiterror Act*, N.Y. TIMES, Jan. 27, 2004, at A1). Unlike the conclusions regarding intent, these decisions (which purport to find vagueness in words of common usage) are highly suspect and, given the interpretation of intent adopted, unnecessary.

146. Some are concerned, for example, with the provisions of Section 216, which amends the pen register/trap and trace statute to clarify that it applies to internet communications, and to allow for a single order that is valid across the country. But for years, law enforcement has used pen registers to track which numbers a particular telephone dials. *See* 18 U.S.C. § 3123. Section 216 again simply updates the law to the technology. It "ensures that law enforcement will be able to collect non-content information about terrorists' com-

dominant area in which they arise lies in information gathering programs being developed outside the four corners of the text of the Patriot Act.

Initially, these concerns first arose in the context of a research program know as Terrorism Information Awareness (TIA).[147] Those concerns have since led Congress to kill the research funding for the proposal.[148] With the end of the TIA program, attention has now turned to the Transportation Security Administration's proposal to use an enhanced information technology program to screen airplane passengers. That program, known as CAPPS II, would effectively conduct a computerized screen of every passenger to assess his or her potential threat as a terrorist.[149]

1. CAPPS II – The System

Since September 11th, the aviation industry has undergone many changes to strengthen airport security. The TSA was created and placed in charge of passenger and baggage screeners (who are now federal employees). It has been using explosives detection systems on 90 percent of checked baggage and substantially expanded the Federal Air Marshal Service. However, little has been done to determine whether a person seeking to board an aircraft belongs to a terrorist organization or otherwise poses a threat. In order to meet this objective, the Transportation Security Administration is developing the Computer Assisted Passenger Prescreening System II (CAPPS II).

---

munications regardless of the media they use." Dept. of Justice, *supra* note 93, at 17. Under long-settled Supreme Court precedent, the use of pen registers does not constitute a "search" within the meaning of the Fourth Amendment. As such, law enforcement need not obtain court approval before installing a pen register. This is so because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," and "when he used his phone, petitioner voluntarily conveyed numerical information to the telephone company." Smith v. Maryland, 442 U.S. 735, 744 (1979). There is little good reason not to apply the same reasoning to internet addresses in the "Send" line of an e-mail.

147. For a detailed discussion of TIA, how it might have worked, and what appropriate legal mechanisms for its control might have been, *see* Paul Rosenzweig, *Proposals for Implementing the Terrorism Information Awareness System*, LEGAL MEMORANDUM NO. 8 (The Heritage Foundation, Aug. 2003), *reprinted in* GEO. J.L. & PUB. POL. (2004) (forthcoming); Taipale, *supra* note 35.

148. S. Amdt. 59 to H.J. Res. 2, Pub. L. No. 108-7 (prohibiting funding for TIA); *see also* Paul Rosenzweig, Michael Scardaville & Ha Nguyen, *Senate Should Restore TIA Funding*, WEB MEMO NO. 315, (The Heritage Foundation, July 2003).

149. This summary of CAPPS II is derived from Paul Rosenzweig & Ha Nyguen, *CAPPS II Should be Tested and Deployed*, BACKGROUNDER NO. 1683 (The Heritage Foundation, Aug. 2003).

Most of the changes made in airport security have focused on looking for potential weapons (better examination of luggage, more alert screeners) and creating obstacles to the use of a weapon on an aircraft (reinforced cockpit doors, armed pilots, etc). A computer-aided system would improve the TSA's ability to assess the risk a passenger may pose to air safety.

The current, limited CAPPS was first deployed in 1996 by Northwest Airlines. Other airlines began to use CAPPS in 1998, as recommended by the White House Commission on Aviation Safety and Security (also known as the Gore Commission).[150] In 1999, responding to public criticism, the FAA limited the use of CAPPS to checked luggage screening. In other words, since 1999, CAPPS information has not been used as a basis for subjecting passengers to personal searches and questioning. As a consequence, even if CAPPS flagged a high-risk passenger, he could not be singled out for more intensive searches.

After September 11th, CAPPS returned to its original conception and is now again used to screen all passengers along with their carry-on and checked luggage. However, the criteria used to select passengers, such as last-minute reservations, cash payment, and short trips are over inclusive. They can flag up to 50% of passengers in some instances, many in short haul markets.[151] Nor does CAPPS attempt to determine whether or not the federal government has information that may connect a specific perspective passenger with terrorism or criminal activity that may indicate they are a threat to the flight. As a result, it's likely that if Osama bin Laden tried to board a plane today, CAPPS would not identify him for arrest or further inspection.[152]

The Transportation Security Agency (TSA) believes that screening what a passenger is carrying is only part of the equation and is developing CAPPS II as a successor to CAPPS in order to deter-

150. *See* White House Commission on Aviation Safety and Security, Feb. 12, 1997, *available at* http//www.airportnet.org/depts/regulatory/gorefinal.htm.

151. *See* Robert W. Poole, Jr. & George Passatino, *A Risk-Based Airport Security Policy*, REASON PUB. POL'Y INST., May 2003, at 11.

152. It has been reported that the CAPPS I system was partially effective, flagging nine of the 19 September 11th terrorists for additional screening. *See* National Commission on Terrorist Attacks Upon the United States, *The Aviation Security System and the 9/11 Attacks: Staff Statement No. 3*, Jan. 27, 2004, *available at* http://www.9-11commission.gov/hearings/hearing7/ staff_statement_3.pdf; *see also* Sara Goo & Dan Eggen, *9/11 Hijackers Used Mace and Knives, Panel Reports*, WASH. POST, Jan. 28, 2004, at A1 (summarizing report). To the extent that is true, it emphasizes both that some form of screening can be effective and that however effective it might be, the human element will always be a factor in insuring the success of any system.

mine whether the individual poses a threat to aviation security. CAPPS II will use government intelligence and law enforcement information in order to assign risk levels to passengers based on real information not arbitrary models. The TSA will then be able to devote more of its resources to those with a higher score (indicating they pose a greater risk), than those deemed to be a lesser concern (although some degree of randomness will need to be retained).

In January 2003, TSA released a Privacy Act notice for CAPPS II, the successor to CAPPS.[153] Since then, many critics have raised substantial concerns. Some thought that CAPPS II was too broad in scope and could infringe on passengers' privacy. Others were concerned that the government should not rely on potentially flawed commercial data to prevent individuals from traveling by air. Some asserted that the use of knowledge discovery technologies on a wide variety of personal data could pose privacy and civil liberty violations. Finally, many wondered if individuals would be able to challenge their score.

TSA has recently made available an Interim Final Privacy Notice on CAPPS II, which includes substantial modifications to the initial proposal based on many of the concerns voiced in response to the first Privacy Notice.[154]

Under the Interim Notice, TSA will not keep any significant amount of information after the completion of a passenger's itinerary. Furthermore, TSA anticipates that it will delete all records of travel for U.S. citizens and lawful permanent residents a certain number of days after the safe completion of the passenger's travels (7 days is the current anticipation). TSA has also committed to developing a mechanism by which a passenger targeted for more thorough screening can seek to set the record straight if they think they have been identified in error.

More importantly, the CAPPS II system has addressed privacy concerns by severely limiting the types of private commercial data that will be examined. The proposed CAPPS II system will access only a "passenger name record" (PNR), which will include information collected at the time the passenger makes the reservations, prior to the flight. Selected PNR information will be transmitted to commercial data providers for the sole purpose of authenticating the passenger's identity. This process is similar to the

153. *See* 68 Fed. Reg. 2101 (Jan. 15, 2003).
154. *See* 68 Fed. Reg. 45265 (Aug. 1, 2003).

credit card application procedure used to check for fraudulent information. Commercial data providers will then transmit back to TSA a numeric score indicating the degree of match between commercial data and TSA data, giving TSA a good idea if the person is who they say they are.[155] No commercial data will be retained by the TSA and no travel data will be retained by the commercial companies.

After the authentication phase, the CAPPS II system will conduct a risk assessment by comparing that identification information to intelligence and law enforcement data. Passengers whose identity is confirmed with a high degree of confidence and have no matches with intelligence or law enforcement data will be less likely to receive additional scrutiny, whereas those on the opposite end of the spectrum will likely be searched more thoroughly or arrested as appropriate. This will allow TSA to focus its prevention resources on those passengers who, through a qualitative analysis, are determined to be more dangerous.[156]

2. *Assessing The Risks of Type I and Type II Errors*

The CAPPS II program poses some interesting and challenging problems in adapting the law to new technology and the realities of new technology to the law.[157] First, if CAPPS II is to be effective, its hallmark will be the idea that some form of "result" will necessarily be immediately available to TSA screeners on a "real-time" basis so that they can make near-instantaneous decisions regarding whom to screen or not screen prior to allowing passengers to board the aircraft. If CAPPS II were designed so that detailed personal information on each passenger were transmitted to every TSA screener, all would agree that the architecture of the system would not adequately protect individual privacy. Thus, the analysis passed by the CAPPS II system to TSA employees at

155. Absolute certainty of identification is impossible. In practice, all identification will be expressed as a "confidence interval" reflecting an estimate of the degree of certainty in an identification. For most travelers, this confidence interval will be quite high. For a few, who will be subject to greater screening, it will not.

156. By all reports, the TSA intends to implement the CAPPS II system this year in one form or another. *See* Sara Goo, *U.S. to Push Airlines for Passenger Records*, WASH. POST, Jan. 12, 2004, at A1. Thus, the issues addressed in this paper are not at all theoretical.

157. This section is derived from earlier Congressional testimony. *See* Paul Rosenzweig, *Can The Use Of Factual Data Analysis Strengthen National Security?*, Testimony Before the United States House of Representatives, Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census (May 20, 2003).

the airport must be limited to a reported color code – red, yellow or green – and should not generally identify the basis for the assignment of the code.

Thus, CAPPS II proposes to precisely reverse the privacy protection equation being developed in other contexts. To protect privacy, other information technology programs disaggregate analysis from identity by making the data available to the analyst while concealing the identity of the subject of the inquiry unless and until disclosure is warranted. In the reverse of this paradigm, CAPPS II will disclose the identity of the potential threat (through a red/yellow/green system displayed to the screener, warning of a particular individual) but will conceal from the screener the data underlying the analysis – again, until such time as a determination is made that the two pieces of information should be combined. The privacy protection built into CAPPS II is therefore the mirror image of the more common system. It is by no means clear which method of protecting privacy is *ex ante* preferable – but it is clear that the two systems operate differently and if we are to have any sort of CAPPS II system at all, it can only have privacy protections of the second kind.

To reiterate a point made earlier, CAPPS II is not necessarily a decrease in privacy. Rather, it requires trade-offs in different types of privacy. It substitutes one privacy intrusion (into electronic data) for another privacy intrusion (the physical intrusiveness of body searches at airports). And it may have the salutary effect of reducing the need for random searches and eliminate the temptation for screeners to use objectionable characteristics of race, religion, or national origin as a proxy for threat indicators.[158] For many Americans, the price of a little less electronic privacy might not be too great if it resulted in a little more physical privacy, fewer random searches, and a reduction in invidious racial profiling.

Finally, the unique subject matter of the CAPPS II system calls for heightened sensitivity to the potential for an infringement on

158. Some purely random searches will need to be maintained in order to maintain inspection system and defeat so-called "Carnival Booth" attacks (named after a student algorithm proposing a method of defeating CAPPS). Adding a random factor to the inspection regime answers the problem. *See* Samidh Chakrabati & Aaron Strauss, *Carnival Booth: An Algorithm for Defeating the Computer-assisted Passenger Screening*, *available at* http://www.swiss.ai.mit.eud/6805/student-papers/spring02-papers/caps.htm (describing program); Taipale, *supra* note 35, at n.281 (explaining how addition of random screening guards against such attacks).

protected constitutional liberties. While the Constitution affords no additional protection to information that an individual has made available to other individuals or institutions, CAPPS II implicates at least two fundamental liberty interests guaranteed by the Constitution. Most obviously, since the 1960's, the Supreme Court has recognized a fundamental right to travel[159] – indeed, one might reasonably say that one significant purpose of the Federal union was to insure the freedom of commerce and travel within the United States. Second, like the FBI Guidelines discussed earlier, many of the indicators that *might* be used to identify potential terrorists are also indicators that, in other circumstances, are potentially the products of protected First Amendment activity – in other words, though CAPPS II is not intended to impinge upon free political speech, it may collaterally do so.

Thus, there is a significant risk that a poorly designed system will impinge upon fundamental constitutional liberties. The risk of such impingement should not result in abandonment of the program – especially not in light of the potentially disastrous consequences of Type II error, another terrorist attack in the United States. However, as with the FBI Guidelines, we will need stringent oversight to provide the requisite safeguards for minimizing inadvertent infringements of civil liberty in the first instance and correcting them as expeditiously as possible.

CAPPS II is therefore a paradigm for answering the question of whether or not we can conceive of a suitable oversight mechanism that would appropriately constrain executive authority while allowing its application to circumstances we consider necessary. As with the FBI guidelines, the use of CAPPS II should be subject to significant Congressional oversight, again including spot checks (in a classified means, if necessary) to insure that the CAPPS II methodology is not being misused. Though the details would need, of course, to be further developed, the outline of such an oversight system might include some or all of the following components:

- CAPPS II should be constructed to include an audit trail so that its use and/or abuse can be reviewed;

- It should not be expanded beyond its current use in identifying suspected terrorists and threats to national

159. Shapiro v. Thompson, 398 U.S. 618 (1969).

security – it should not be used as a means, for example, of identifying drug couriers or deadbeat dads.[160] Thus, the pending proposal to screen for outstanding criminal warrants should be rejected;

• The program should sunset after a fixed period of time, thereby ensuring adequate Congressional review;

• CAPPS II should have significant civil and criminal penalties for abuse.

• The "algorithm" used to screen for potential danger must, necessarily, be maintained in secret, as its disclosure would frustrate the purpose of CAPPS II. It must, however, also be subject to appropriate congressional scrutiny in a classified setting and, if necessary, independent (possibly classified) technical scrutiny;

• An individual listed for additional screening or prohibited from flying should be entitled to know the basis for his or her listing and should have a mechanism for challenging the listing before a neutral arbiter or tribunal. To the extent practicable, the review should be as prompt as possible;

• Because commercial databases may be error-ridden, no American should be totally denied a right to travel (i.e. red-carded) and subject to likely arrest as a suspected terrorist solely on the basis of public, commercial data. An indication of threat sufficient to warrant denial of that right should (except in extraordinarily compelling circumstances) be based only upon significant intelligence from non-commercial sources.

• The CAPPS II system should be designed so that the No-Fly/Red Card designation, though initially made as the product of a computer algorithm, is never transmitted to the "retail" TSA screening system until it has been reviewed and approved by an official of sufficiently high authority within TSA to insure accountability for the sys-

160. *Cf.* William Stuntz, *Local Policing After the Terror*, 111 YALE L.J. 2183, 2184 (use of expanded surveillance authority to prosecute only terrorists and other serious offenses).

tem.[161] Nor is there any reason for the underlying data ever to be transmitted to the TSA screener.

Finally, before full deployment, CAPPS II needs to demonstrate its effectiveness. It holds great promise – but promise is far different from reality. Indeed, thoughtful critics have identified at least one potentially significant hole in the proposed screening system – it does not account for identity theft.[162] Thus, while the technology will allow the resolution of an identity – that is determining whether the identity is a false, created one or not – it cannot resolve the theft of a true identity. Given the limited amount of information being requested (name, address, date of birth, and telephone number) it is quite likely that individuals could pose as people other than themselves readily. It takes little more than a few hours in a coffee shop, overhearing conversations, to make it likely that enough information could be gathered to pose as someone else. And the only ways to enhance CAPPS II to fight this prospect are to strengthen it -- either by collecting additional information about an individual or to return additional information (for example, gender, height, weight and hair color) to the TSA

161. This would mirror the view of the European Union which styles it as a "right" to have human checking of adverse automated decisions. The EU Directives may be found *at* http://www.dataprivacy.ie/6aii-2.htm#15.

162. Other critics are more skeptical, characterizing CAPPS II as the search for a "silver bullet" that cannot work because of Bayesian probability problems. *E.g.*, ROSEN, *supra* note 29, at 105-06. That broad statistical criticism is rejected by researchers in the field who believe that because of the high correlation of data variables that are indicative of terrorist activity, a sufficient number of variables can be used in any model to create relational inferences and substantially reduce the incidence of false positives. *See* Remarks, David Jensen, *Data Mining in the Private Sector*, Center for Strategic and International Studies, July 23, 2003; David Jensen, Matthew Rattigan, Hannah Blau, *Information Awareness: A Prospective Technical Assessment*, SIGKDD '03 (Aug. 2003) (ACM 1-58113-737-0/03/0008). To be sure, the ultimate efficacy of the technology developed is a vital antecedent question. If the technology proves not to work—if, for example, it produces 95 percent false positives in a test environment—than all questions of implementation may be moot. For no one favors deploying a new technology—especially one that threatens liberty—if it is ineffective. It is important to recognize, however, that CAPPS II is a test project – thus, we are unwise to reject it before knowing whether the effectiveness problem can be solved. It is also important to realize that there may be potentially divergent definitions of "effectiveness." Such a definition requires *both* an evaluation of the consequences of a false positive *and* an evaluation of the consequences of failing to implement the technology. If the consequences of a false positive are relatively modest (e.g. enhanced screening), and if the mechanisms to correct false positives are robust (as recommended herein), then we might accept a higher false positive rate precisely because the consequences of failing to use CAPPS II technology (if it proves effective) could be so catastrophic. In other words, we might accept 1,000 false positives if the only consequence is heightened surveillance and the benefit gained is a 50 percent chance of preventing the next terrorist flight attack. The vital research question, as yet unanswered, is the actual utility of the system and the precise probabilities of its error rates.

screener so that the screener could confirm the identity of the individual before him or by requiring travelers to use some verified token or identification with clearance incorporated in it.[163] These are neither technologically easy nor necessarily desirable results – yet the conundrum of identity theft must be solved if CAPPS II is to prove at all useful.[164]

On the whole, however, we should welcome the attempt to develop CAPPS II technology. Enhanced technology allowing the correlation of disparate databases and information has potentially significant positive uses. American troops in Iraq, for example, use the same sorts of link and pattern analysis, prediction algorithms and enhanced database technology that would form a part of CAPPS II (and formed a part of TIA) to successfully track the guerrilla insurgency.[165]

In short, the proposed system has, as noted, some significant holes that need to be closed. But failing to make the effort to use new technology wisely poses grave risks and is an irresponsible abdication of responsibility. As six former top-ranking professionals in America's security services recently observed, we face two problems—both a need for better analysis and, more critically, "improved espionage, to provide the essential missing intelli-

---

163. *See* K. A. Taipale, *Identification Systems and Domestic Security: Who's Who in Whoville,* Potomac Institute for Policy Studies, Jan. 28, 2003, *available at* http://www.stilwell.org/presentations/CAS-IDsystems-012804.pdf.

164. One could also take steps to harden identification cards to ensure they are less readily falsifiable and more certainly government products. *See* Markle Foundation, *Task Force on National Security in the Information Age, App. A "Reliable Identification for Homeland Protection and Collateral Gains"* (Dec. 2003) (recommending hardened drivers license identification). Such hardening will not, however, be of great utility unless we also strengthen the authentication process to insure that those seeking identification are who they say they are. Colorado's recent adoption of a biometric face identification mechanism offers some promise of a technological solution to that question. *See State of Colorado Deploys Facial Recognition Technology to Fight Identity Theft* (Digimarc 2003) (on file with author) (reporting detection of 20 attempted frauds per month through facial recognition technology).

165. *See* AP, *Computer-sleuthing aids troops in Iraq*, Dec. 23, 2003. Any who doubt that, in some form, enhanced information search technology can work need only contemplate the recent arrest of LaShawn Pettus-Brown, whose date identified him as a fugitive when she "Googled" him. *See* Dan Horn, *Fugitive Done in by Savvy Date and Google,* USA TODAY, Jan. 29, 2004, *available at* http://www.usatoday.com/tech/news/2004-01-29-google-bust_x.htm. Compare that with the pre-September 11th prohibition (eliminated by the FBI guidelines discussed, *supra*) on the FBI's use of Google. *See* L. Gordon Crovitz, *Info@FBI.gov*, WALL ST. J., June 5, 2002. At some fundamental level, the ultimate question is how to reconcile readily available technology in commercial and public use, with the broad governmental monopoly on the authorized use of force. Whatever the proper resolution, we cannot achieve it by hiding our heads in the sand and pretending that data integration technology does not exist.

gence." In their view, while there was "certainly a lack of dot-connecting before September 11th," the more critical failure was that "[t]here were too few useful dots."[166] CAPPS II technology can help to answer both of these needs. Indeed, resistance to new technology poses practical dangers. As the Congressional Joint Inquiry into the events of September 11th pointed out, in noting systemic failures that played a role in the inability to prevent the terrorist attacks:

> 4. Finding: While technology remains one of this nation's greatest advantages, it has not been fully and most effectively applied in support of U.S. counterterrorism efforts. Persistent problems in this area included a lack of collaboration between Intelligence Community agencies [and] *a reluctance to develop and implement new technical capabilities aggressively* . . . .[167]

Or, as one commentator has noted, the reflexive opposition to speculative research by some members of Congress and the public is "downright un-American."[168] It is an example of the "zero defect" culture of punishing failures, not reason. Though CAPPS II technology might prove unavailing, the only certainty at this point is that no one knows. It would be particularly unfortunate if America's elected leaders opposed basic scientific research without the least sense that in doing so they demonstrate a "lack [of] the essential American willingness to take risks, to propose outlandish ideas and, on occasion, to fail."[169] That flaw is the way to stifle bold and creative ideas—a "play it safe" mindset that, in the end, is a disservice to American interests.

III. CONCLUSION

The Patriot Act has become something of a political football in the past few months. One sees television commercials of anony-

166. Robert Bryant et al., *America Needs More Spies*, ECONOMIST, July 12, 2003, at 30.

167. *Report of the Joint Inquiry Into the Terrorist Attacks of September 11, 2001*, House Permanent Select Committee on Intelligence and Senate Select Committee on Intelligence, 107th Cong., 2nd Sess., S. Rept. No. 107–351 and H. Rept. No. 107–792, Dec. 2002, p. xvi, *available at* http://www.fas.org/irp/congress/2002_rpt/911rept.pdf (emphasis supplied). The Joint Inquiry also critiqued the lack of adequate analytical tools, *id.* at Finding 5, and the lack of a single means of coordinating disparate counterterrorism databases, *id.* at Findings 9 & 10. Again, aspects of the CAPPS II program are intended to address these inadequacies and limitations on the research program are inconsistent with the Joint Inquiry's findings.

168. *See* David Ignatius, *Back in the Safe Zone*, WASH. POST, Aug. 1, 2003, at A19.

169. *Id.*

mous hands ripping up the Constitution, with a voice-over blaming Attorney General Ashcroft. Print ads show an elderly gentleman leaving a bookstore with text decrying the use of government powers to get his book purchase list. But the hysteria is somewhat overblown.

Nobody would seriously dispute the major premise of Chief Justice Rehnquist's analysis – an analysis echoed by Judge Richard Posner:[170] in assessing the appropriateness of infringements on American liberty, we must take into account the severity of the threat being averted. In this time of terror, some adjustment of the balance between liberty and security is both necessary and appropriate. And, as the courts are likely to agree, the Constitution is sufficiently malleable and pragmatic to accommodate this balancing of interests. Indeed, the very text of the Fourth Amendment – with its prohibition only of "unreasonable" searches and seizures – explicitly recognizes the need to balance the harm averted against the extent of governmental intrusion.

But in combating the increased threat to public safety, we must take care not to systematically undervalue the countervailing liberty interest.[171] Our history suggests precisely why this risk exists: the insidious contraction of liberty results from measures taken with the best intentions, not malevolent ones. As Judge Posner writes, at the time the internment of Japanese Americans seemed like a reasonable attempt to ensure public safety. Yet, in retrospect, all agree that in placing so great a priority on public-safety interests, the government acted unjustly and without sufficient regard for the liberty interests of the Japanese-American citizens.

It may well be that liberty must be curtailed when the public need is great enough. But, at a minimum, we should interpret the Constitution as embodying a cautionary rule: public safety should be effectuated through the least intrusive means possible, allowing maximum scope for personal liberty.

How, then, should we approach the practical questions of governmental conduct arising in a post-September 11 world? With our eyes wide open and with a dose of healthy skepticism. The good news is that we have plenty of both. Courts and the Con-

170. Judge Richard Posner, *The Truth about Our Liberties*, THE RESPONSIVE COMMUNITY, Summer 2002, at 4.

171. Paul Rosenzweig, *A Watchful America*, THE RESPONSIVE COMMUNITY, Fall 2002, at 89.

gress are casting a jaundiced eye at the administration's more extravagant and overblown proposals for reform, while accommodating and expediting the more urgent and reasonable requests. Already, for example, the courts have rejected governmental claims to the detention hearings secret and begun to scrutinize the closing of immigration hearings and the indefinite detention of individuals as material witnesses or unlawful combatants.[172] The press has accepted the challenge of fulfilling its traditional function as a check on authoritarian excess. Most importantly, the pendulum of public opinion has steadied as the initial shock of terrorism wears off. The American public instinctively understands that prudential adjustments during times of crisis do not (and should not) reset the balance between liberty and security permanently. Once the necessity of war has lapsed, we anticipate a return to the general rule of constitutional liberty.

Thomas Jefferson said: "The natural progress of things is for liberty to yield and government to gain ground."[173] While accommodating the need for government to ensure domestic tranquility in these troubled times, a watchful America can guard against this natural tendency.

But it cannot do so with an over-wrought sense of fear. Most of the steps proposed to combat terror have already been used to combat organized crime. And there is little evidence of any real abuse.[174] No First Amendment liberties have been curtailed, no dissent or criticism suppressed.[175] While Jefferson was right that we must be cautious, John Locke, the seventeenth-century philosopher who greatly influenced the Founding Fathers, was equally right when he wrote: "In all states of created beings, capable of laws, where there is no law there is no freedom. For liberty is to be free from the restraint and violence from others; which cannot be where there is no law; and is not, as we are told, a liberty for every man to do what he lists."[176] Thus, the obligation of

172. *E.g.*, Detroit Free Press v. Ashcroft, 303 F.3d 681 (6th Cir. 2002) (requiring immigration detention hearings to be open); North Jersey Media Group, Inc. v. Ashcroft, 308 F.3d 198 (3d Cir. 2002) (allowing detention hearings to be closed upon particularized showing); U.S. v. Awadalah, 349 F.3d 49 (2d Cir. 2003) (allowing detention of material witnesses for grand jury investigation); *see also supra* note 31 (review of detention of enemy combatants and Guantanamo Bay detainees).

173. Letter to E. Carrington, May 27, 1788, reprinted in THE FOUNDERS' ALMANAC, *supra* note 75, at 157.

174. *See supra* note 6.

175. *See* Chertoff, *supra* note 28, at 16 (making this claim). Critics can point to little, if any, evidence rebutting this assertion.

176. JOHN LOCKE, TWO TREATISES OF GOVERNMENT 305 (Peter Laslett, ed., 1988).

the government is a dual one: to protect civil safety and security against violence *and* to preserve civil liberty.

The time to address these issues is now. As Michael Chertoff, the former Assistant Attorney General for the Criminal Division, has written:

> The balance [between liberty and the response to terror] was struck in the first flush of emergency. If history shows anything, however, it shows that we must be prepared to review and if necessary recalibrate that balance. We should get about doing so, in light of the experience of our forbearers and the experience of our own time.[177]

Others have echoed that call.[178] But in reviewing what we have done and what we should do in the future, we must be guided by the realization that this is not a zero-sum game. We can achieve both goals – liberty and security – to an appreciable degree. The key is empowering government, while exercising oversight. So long as we keep a vigilant eye on police authority, so long as the federal courts remain open, and so long as the debate about governmental conduct is a vibrant part of the American dialogue, the risk of excessive encroachment on our fundamental liberties is remote. The only real danger lies in silence and leaving policies unexamined.

177. Chertoff, *supra* note 28, at 17.

178. *E.g.*, Susan Schmidt, *Bipartisan Debate on Patriot Act is Urged*, WASH. POST, Nov. 14, 2003 (former Deputy Attorney General Thompson proposes bipartisan commission to debate "the legal tools that should be employed in combating terrorism").