

## Chapter 4

---

# After the Patriot Act

**T**he cold truth is that we cannot always trust the people that work for us. For over fifty years, J. Edgar Hoover served as director of the FBI. He also spied on Americans for no good reason.

From the presidency of Calvin Coolidge to that of Richard Nixon, Hoover ran the chief U.S. agency responsible for fighting terrorism on American shores. From its inception, the FBI was always concerned about tracking down criminals and provocateurs. In 1918, one year after the Russian Revolution, fear about the threat of anarchists and Communists (the latter called the “Red Scare”) grew after an attempted bomb attack against the U.S. Attorney General. Congress rushed through \$500,000 in funding for a new anti-radical unit in the Department of Justice’s Bureau of Investigation—led by a young official named J. Edgar Hoover.

In early 1920, federal agents conducted raids across the nation, taking thousands of suspected radicals—many of them immigrants—into custody and prompting an outcry from civil libertarians.<sup>1</sup> In 1939, the FBI used secret wiretaps, not only to keep tabs on Fifth Columnists, pro-Nazi groups, and Communists, but also to gather detailed political intelligence about President Roosevelt’s anti-interventionist critics. The agency continued to pass on information about FDR’s political enemies throughout the war.<sup>2</sup> However, the FBI’s greatest abuses were saved for the Cold War when the agency pursued civil rights and anti-war activists under the guise of a counter-communist crusade. (See Appendix 8.)

After 55 years of searching for secrets, Hoover died in his bed on May 2, 1972. Until that time, he was still running the agency he founded: an agency that had taken on bootleggers and bank robbers, the mob and money launders, spies and saboteurs—and everyday Americans. President Nixon ordered a state funeral, even as Hoover’s carefully cultivated image as the all-American “G-Man” was already under attack. In 1968, Congress passed a law requiring Senate confirmation of FBI directors and limiting their terms to 10 years. Meanwhile, as J. Edgar Hoover went to his final rest at Washington’s Congressional Cemetery, Americans turned their attention to a crime the FBI had largely ignored—a burglary at the Watergate.

Although U.S. strategy during the Cold War often achieved all three of its priorities (adequate security, economic growth, and a strong civil society), it was far from perfect in execution. The excesses committed in the process of chasing the enemies hiding among us were a case in point. In the Cold War era, the legal structures designed to combat communism were, at times, effective, but were frequently overly intrusive. To enhance our ability to investigate potential domestic Communist influences, we too readily granted new investigative authority to the FBI and CIA—authority that was sometimes abused. To incapacitate domestic opponents we painted with a broad brush. At times, for example, communism was outlawed altogether. Meanwhile, neither Congress, the courts, nor the public paid much attention. The abuses of the executive branch ran unexamined and unchecked for over a decade. We can do better.

The answer is simple. We need enhanced investigative authorities, but none so broad as to become a license for abuse. We need a means of incapacitating those who would do injury to America, but in a manner that does not threaten cherished freedoms. We need to put into place an oversight mechanism that works—one that allows us to empower the executive to combat terrorism, while at the same time preventing abuse.

## Looking for Mr. Terrorist

“Business as usual” will not stop twenty-first century terrorism. We need to do things differently. The first step that needs to be taken is to move forward on the successful initiatives that have already been undertaken.

During the well-publicized hearings of the 9/11 Commission, present and former government officials from both the Clinton and Bush Administrations,



President Lyndon B. Johnson speaks in denunciation of the Ku Klux Klan. At left: FBI Director J. Edgar Hoover. (PHOTO COURTESY OF THE NATIONAL ARCHIVES)

Republicans and Democrats, acknowledged that prior to 9/11 a “wall” of legal and regulatory policies prevented effective sharing of information between the intelligence and law enforcement communities. Attorney General John Ashcroft noted that in 1995 the Justice Department embraced legal reasoning that effectively excluded prosecutors from intelligence investigations. At times, for prudential reasons, Justice Department officials even raised the “wall” *higher* than was required by law, to avoid any appearance of “impermissibly” mixing law enforcement and intelligence activities.

Indeed, a very real wall existed. It was based on a standard that allowed the use of intelligence-gathering mechanisms only when foreign intelligence was the “primary purpose” of the activity. This old “primary purpose” standard derived from a series of court decisions. The standard was formally established in written Department of Justice guidelines in July 1995. Although 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 cases.



FBI employee coding fingerprints. (COURTESY OF THE NATIONAL BUREAU OF STANDARDS)

The old legal rules discouraged coordination and created what the Foreign Intelligence Surveillance Court of Review calls “perverse organizational incentives.”<sup>3</sup> The wall had some very negative real-world consequences. Former Department of Justice official Victoria Toensing tells of one: In the 1980s, terrorists hijacked an airplane, TWA Flight 847, which eventually landed in Lebanon. At the time that negotiations were ongoing, the FBI had the capacity to intercept 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 dumped his body onto the airport tarmac on live TV. As a result, the Department of Justice announced its intention to capture and prosecute those responsible, which had the immediate effect of making the FBI’s ongoing intercepts no longer for the “primary” purpose of foreign intelligence gathering: The “primary” purpose was now clearly prosecution. As a result, in the middle of a terrorist crisis, the FBI turned *off* its listening devices for fear of violating the rule against using intelligence-gathering techniques in a situation in which intelligence gathering was not the main purpose. It is difficult to conceive of a more wrongheaded course of conduct, yet the FBI, rightly, felt that it was legally required to act as it did.

Nor is this the only instance in which the artificial “wall” has deterred vital information sharing between the 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 9/11. Instead, the culture against information sharing was so deeply ingrained that during the criminal prosecutions for the 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.<sup>4</sup> There is even some possibility that this wall may have been the contributing factor to our failure to prevent the 9/11 attacks.

Largely in response to these problems, Congress passed the USA Patriot Act subsequent to the September 11 attacks. As Viet Dinh (one of the act’s principal authors) concluded, the law “makes the best use of the information we have, sharing information between law enforcement agencies to put the pieces of the puzzle together so we can look for the needle in the haystack.”<sup>5</sup> Not only was the legislation needed, it has proved its worth in practice. The law has facilitated dozens of reported terrorist investigations by removing both real and imagined barriers that kept the people trying to protect us from working together. To date, as the Department of Justice Inspector General has reported, there has not been one single instance of abuse of the powers granted in the act.

Safeguarding the civil liberties of American citizens is vitally important, as important during war as during periods of peace. Yet so, too, is preserving our security. The Patriot Act preserves both. Hysterical criticisms that the act was unnecessary and is a threat to a healthy civil society have proven unfounded, and calls for repeal or significant revision are misguided.

Thus, we reject the broadest criticisms of the Patriot Act: 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 “wish list” of law enforcement powers.

In particular, one aspect of the Patriot Act, embodied in Sections 203 and 218, was absolutely vital. (See Appendix 9.) Section 203 permits law enforcement information gathered through a grand jury investigation to be shared with intelligence agencies. Section 218 allows the use of intelligence information-gathering mechanisms whenever intelligence gathering is a “significant” purpose of an investigation—and it allows the information gathered

to be shared with law enforcement. Taken together, these two sections effectively tear down the “wall” that existed between law enforcement and intelligence agencies and permit inter-agency cooperation.

Sections 203 and 218 empower federal agencies to share information on terrorist activity. This is an important, significant, and positive development. One of the principal criticisms made in virtually every review of our pre-September 11 actions is that we failed to “connect the dots.” Indeed, as a 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.”<sup>6</sup>

In short, the Patriot Act changes (as a general principle) adopt 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 once imposed on such information sharing are the relics 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 on charges of providing material support to several Palestinian terrorist organizations. The government’s case against Al-Arian is apparently based on foreign counterintelligence wiretap intercepts that date back as far as 1993. According to the information in those wiretaps, 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. That information has been in the possession of our intelligence organizations for at least the past seven 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 legally allowed to provide that information to law enforcement officials. Only those changes allowed the government to file the charges pending against Al-Arian. As the Al-Arian case suggests, 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.

Nor can it be convincingly argued that these changes violate the Constitution. To the contrary, as the Court of Review made clear, a wall between

intelligence and law enforcement is not constitutionally required. 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.”<sup>7</sup> The courts and Congress agree that appropriate information sharing is simply the right thing to do.

## Roving Wiretaps

Other aspects of the Patriot Act are also worth preserving. Section 206, for example, authorizes the use of “roving wiretaps” in terrorist investigations—that is, wiretaps that follow an individual and are not tied to a specific telephone or location. America’s original electronic surveillance laws (the Foreign Intelligence Surveillance Act and Title III of the Omnibus Crime Control Act of 1968) stem from a time when phones were the only means of electronic communications and all phones were connected by hard wires to a wall outlet.

Roving wiretaps have arisen over the past twenty years for use in the investigation of many crimes (e.g., drug transactions or organized crime activities) because modern technologies (cell phones, BlackBerries, and Internet telephony) allow those seeking to evade detection the ability to change communications devices and locations at will.

Here is an outline of the general structure of laws governing when law enforcement or intelligence agents may conduct electronic surveillance relating to suspected foreign intelligence or terrorism activity. Title III of the Omnibus Crime Control Act of 1968 (which governs electronic surveillance for domestic crime) allows a court to enter an order authorizing electronic surveillance if “there is probable cause for belief that an individual is committing, has committed or is about to commit” one of a list of several specified crimes.

The Foreign Intelligence Surveillance Act (or FISA—the statute governing intelligence and terrorism surveillance) has a parallel requirement: A warrant may be issued if there is probable cause to believe that the target of the surveillance is a foreign power or the agent of a foreign power. FISA also requires that the government establish probable cause to believe that “each of the facilities or places at which the surveillance is directed is being used, or is about to be used” by the foreign power or the agent of the foreign power who

is the target of surveillance. Thus, FISA court warrants are issued by federal judges upon a showing of probable cause, and they describe the things to be seized with particularity—the traditional requirement contained in the Fourth Amendment.

Thus, no one can argue that these FISA warrants violate the Constitution. To the contrary, as the Foreign Intelligence Surveillance Court of Review recently made clear, the FISA warrant structure 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.” This is so because, as the court recognized, 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 people from committing crimes. The government’s concern with respect to foreign intelligence crimes, on the other hand, is overwhelmingly to stop or frustrate the immediate criminal activity before it happens.

Roving wiretaps (whether used in foreign intelligence or domestic criminal investigations) are a response to changing technologies. Phones are no longer fixed in one place and can move across state borders at the speed of flight. Sophisticated terrorists and criminals can change phones and communications devices constantly in an attempt to thwart interception.

In response to these changes in technology, in 1986 Congress authorized a change in the requirement for the investigation of drug offenses. Under the modified law, the authority to intercept an individual’s electronic communication was tied to the individual who was the suspect of criminal activity (and who was attempting to “thwart” surveillance), rather than to a particular communications device.

Section 206 of the Patriot Act authorized the same techniques for foreign intelligence investigations. As the Department of Justice has noted: “This provision has enhanced the government’s ability to monitor sophisticated international terrorists and intelligence officers, who are trained to thwart surveillance by rapidly changing hotels, cell phones, and internet accounts, just before important meetings or communications.”

One important safeguard is that the FISA court may authorize such roving wiretaps *only* if it makes a finding as to the terrorist’s actions—that “the actions of the target of the application may have the effect of thwarting the identification” of a terrorism suspect. With that safeguard, this tool (already

in use for drug crime investigations) is perfectly appropriate for terrorism investigations as well.

## **“Sneak and Peek” Warrants**

The same is true of another section of the Patriot Act that has engendered great criticism. Section 213 authorizes the issuance of delayed notification search warrants, which critics call “sneak and peek” warrants. Traditionally, when the courts have issued search warrants allowing the government’s forcible entry into a citizen’s home or office, they have required that the searching officers immediately notify the individual whose home or office has been entered. Prior to September 11, 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. Yet here, too, the fears of abuse seem to outstrip reality.

Delayed notification warrants are a longstanding crime-fighting tool upheld by courts nationwide for decades in instances of 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. Yet the seizure would have been useless without a way of breaking the encryption. Therefore, using a delayed notification warrant, the FBI secretly placed a keystroke logger on Scarfo’s computer. The logger recorded Scarfo’s password, which the FBI then used to examine Scarfo’s records of various drug deals and murders. It would, of course, have been fruitless for the FBI to have secured a warrant to enter Scarfo’s home and place a logger on his computer, if, at the same time, it had been required to notify Scarfo that it had done so.

The courts have approved this common law use of delayed notification. More than twenty 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.”<sup>8</sup> In an earlier case—the seminal case defining the scope of privacy in

contemporary America—the Court said that “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.”<sup>9</sup>

Section 213 of the Patriot Act thus attempts to codify the common law authority given to law enforcement for decades. Now, under Section 213, courts can delay notice if there is “reasonable cause” to believe that immediate notification may have an adverse result, such as allowing a suspect to flee. The “reasonable cause” standard is consistent with pre-Patriot Act case law for delayed notice of warrants. The law goes further, narrowly defining “reasonable cause” for the issuance of a court order. Courts are, under Section 213, allowed to delay notice only when immediate notification may result in an individual’s death or physical harm, flight from prosecution, evidence tampering, witness intimidation, or might otherwise seriously jeopardize an investigation.

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. As 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 that apply to getting a warrant to enter a building in the first place. 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, the presence of oversight rules seems strong, certainly strong enough to prevent the abuse that some critics fear.

Nor can it be doubted that the delayed notification standards 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. In another instance, the Justice Department described a hypothetical situation (based upon an actual case) in which the FBI secured access to the hard drive of terrorists who had sent their computer out for repair. In still another, they were able to plant a surveillance device in a building used by

terrorists as a safe house. All of these are, with adequate safeguards, good uses of a new investigative authority.

## Angry Librarians

Perhaps no provision of the Patriot Act has excited greater controversy than has Section 215, the so-called angry librarians provision.<sup>10</sup> This section allows the Foreign Intelligence Surveillance Court involved in a foreign intelligence investigation to issue an order directing the recipient to produce tangible things such as business records.

The revised statutory authority in Section 215 is not wholly new. Ever since its inception, FISA has had authority for securing some forms of business records. The new statute modifies FISA's original business records authority in 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."<sup>11</sup>

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).'"<sup>12</sup>

Thus, the modifications made by Section 215 do not explicitly allow the production of library records. However, by its terms, it authorizes orders to require the production of virtually any business record. That might include library records, although it would also include such things as airline manifests, international banking transaction records, and purchase records of all kinds.

Like many parts of the Patriot Act, 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 have for years 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. Likewise, 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 books by that poet. 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.

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 obtain a court order. Agents cannot compel any entity to turn over records unless judicial authority has been obtained. In this way, FISA orders are actually better than traditional grand jury subpoenas (which are requested without court supervision and are subject to challenge only after they have been issued).

Second, Section 215 has a narrow scope. It can be used only “to obtain foreign intelligence information not concerning a United States person” or “to protect against international terrorism or clandestine intelligence activities.” It cannot be used to investigate ordinary crimes, or even domestic terrorism. Nor can it be used in any investigation premised solely upon “activities protected by the first amendment to the Constitution.”<sup>13</sup>

This is narrower than the scope of traditional law enforcement investigations. Under general criminal law, the grand jury may seek the production of any relevant business records. The only limitation is that the subpoena may be quashed if the 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.”<sup>14</sup> There is no necessity of showing a connection to foreign intelligence activity, nor any limitation against investigation of United States persons. Thus, unlike under Section 215, the grand jury may inquire into potential violations of any federal crime with effectively limitless authority.

Critics make two particular criticisms of this Section 215: that the judicial review provision is a sham, and that the provision imposing secrecy on the recipients of subpoenas issued pursuant to this section imposes a “gag rule” that prevents oversight of the use of the section’s authority. Neither criticism, however, withstands close scrutiny.

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. This criticism misreads the statute, which, while saying that the subpoena “shall” issue, also says that it shall issue as sought or “as modified.” Thus, the reviewing judge has explicit authority to alter the scope and nature of the request for documents—a power that cannot be exercised in the absence of substantive review of the subpoena request. The suggestion that the provisions of Section 215 prevent judicial review is simply mistaken. To the contrary, Section 215 authorizes judicial review and modification of the subpoena request that occurs prior to issuance of the subpoena. This is a substantial improvement over the situation in traditional grand jury investigations in which the subpoena is issued without judicial intervention and the review occurs at the end of the process—and then only if the subpoena is challenged.

Nor is judicial oversight the only mechanism by which the use of Section 215’s authority is monitored. The section expressly commands that the Attorney General “fully inform” Congress how the section is being implemented. On October 17, 2002, the House Judiciary Committee, after reviewing the Attorney General’s first report, indicated that it was satisfied with the Justice 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.”<sup>15</sup> If it were a problem (for example, if the Department were conducting investigations in violation of the First Amendment based upon the reading habits of suspects), we can be sure that Congress would have said so. That it has not demonstrates that, once again, critics’ fears far outpace reality.

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, but this is a necessary precaution to avoid prematurely disclosing to the subjects of a terrorism investigation that they are subject to government scrutiny. It is also the same rule we apply in drug investigations, with no evidence of abuse. So long as the law is interpreted to allow judicial review, it poses no great danger.

## **Causes for Concern, Causes for Calm**

There are parts of the Patriot Act that do warrant close scrutiny. For example, the “material support” provisions of the Patriot Act make providing material support to terrorists a crime. The problem here is that sometimes the line

between legitimate public speech and actually helping terrorists can be hard to find. There is always the possibility that aggressive use of the law might jeopardize the fundamental right to openly criticize the government.

It could be argued that the actual language of the statute is pretty clear in what it means by material support. Yet it is also clear that an ill-minded government could seek to apply these “clear” words to protected First Amendment conduct. Thus, the concern is not with the body of the statute itself, but with a potentially broad application of the law. However, a simple change can limit the potential for abuse: construing the *scienter* (or intent) requirements in a manner that protects innocent actors. *Scienter* is an element of guilt that has to be proven in order to obtain a conviction. It requires that the accused person have knowledge of the illegality of his or her act. Thus, a person who unknowingly passes a counterfeit coin has not committed a crime. Someone who intentionally hands out fake twenty-dollar bills has. Likewise, an important part of the material support provision is proving that the accused is knowingly helping terrorists.<sup>16</sup>

Although the Patriot Act does not make clear what intent must be proven, it has begun to be interpreted by the courts in a restrictive manner. This demonstrates that we can grant the government additional powers to combat terrorism while reasonably anticipating that the checking mechanisms in place will restrain excessive use of those powers. In addition, juries will help sort this out. Our collective American experience is that juries are quite good at sorting out sham claims of innocence from legitimate ones. Although it appears that there may be sufficient provisions in place to keep abuses in check, we still need to keep an eye on how the material support provision is handled in practice—lest the ghost of Wisconsin slip under the door.

The right answer for addressing concerns over the material support provision (and other parts of the act, as well) is ensuring that we continue to provide the right supervision and control. Part of that supervision will be the judges. Nor are the courts the only oversight mechanism in place. The oversight function of Congress also acts as a direct restraint on executive abuse.

## **FBI Investigative Guidelines**

Another set of law enforcement tools that bear watching are new FBI investigative guidelines<sup>17</sup> issued by the Attorney General in the wake of 9/11.<sup>18</sup> These guidelines are not laws; they are directions from the nation’s chief law

enforcement officer about how to enforce the laws. In short, the new rules authorize FBI agents to open up anti-terror investigations 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. The FBI’s critics wonder if the rules won’t lead to a return of the “bad old days” during the Cold War when domestic intelligence became political spying.

Thus, there is a significant risk that even well-intentioned guidelines won’t stop abusive operations that will impinge upon fundamental constitutional liberties. This does not mean that the risk of abuse requires abandoning new domestic investigations. However, fairly stringent steps are necessary to provide adequate safeguards. Those steps might include 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. As a spot check, Congress should examine individual, closed cases (if necessary, using confidential procedures to maintain classified status) in order to assure itself that the investigative guidelines are not being misused.
- Authorization for “criminal intelligence” investigations under the FBI’s guidelines should, in all circumstances, be in writing so 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.
- 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.

- Additionally, there should be a hesitancy in visiting public places and events that are clearly intended to involve the exercise of core First Amendment rights, because 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 such steps are taken. Conversely, existing court consent decrees that expressly prohibit all such activity (as is currently the case in New York City<sup>19</sup>) should be revisited.
- No American should be the subject of a criminal investigation solely on the basis of his or her 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 now appears, 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. An explicit provision providing for the destruction or archiving (with limited retrieval authority) of these documents might also be prudent.

## **It's the Technology, Stupid!**

There is more to making sure the future is free and safe than the Patriot Act and the FBI's investigatory guidelines. We still need better tools than we have. One answer is technology. New twenty-first century technologies (ranging from data-mining,<sup>20</sup> to link analysis and data-integration, to biometrics,<sup>21</sup> to new encryption techniques) have much to offer in achieving the compelling national goal of preventing terrorism. At the same time, government access to and use of personal information raises concerns about the protection of civil liberties, privacy, and due process. Given the limited applicability of current privacy laws to the modern digital data environment, resolving this conflict will require the adoption of new policies for collection and access, use, disclosure and retention of information, and for redress and oversight.

It is appropriate to begin by asking a practical, concrete question: Can the new technologies be developed, deployed, implemented, and operated in a manner that allows them to be used as an effective anti-terrorism tool while ensuring that there is minimal risk that use of the tool-set will infringe upon American civil liberties?

Some believe this goal is unachievable. Civil libertarians argue that intelligence-gathering technology is a “Big Brother” project that ought to be abandoned. They begin with the truism that no technology is foolproof—every new technology will inevitably generate errors and mistakes will be made. As with the development of any new technology, risks exist for the misuse and abuse of the new tools being developed. From this, critics conclude that the risks of potential error or abuse are so great that development of many new technologies should be abandoned. To buttress the claim that these systems should be abandoned, these critics parade a host of unanswered questions. Among them: Who will operate the systems? What will the oversight be? What will be the collateral consequences for individuals identified as terrorist suspects?

These questions are posed as if they have no answers when all that is true is that for a system under development, they have no answers *yet*. The same is true of any new government program; thus, we know that these implementation issues are generally capable of being resolved.

Yet to hear civil libertarians ask these questions is to suppose that they believe there are no answers. In fact, there are a number of analogous oversight and implementation structures already in existence that can be borrowed and suitably modified to the new technologies. Thus, new enabling technologies can and should be developed if the technology proves usable. This can be done in a way that makes them effective, while posing minimal risks to American liberties, if the system is crafted carefully with built-in safeguards to check the possibilities of error or abuse. There are a number of things that can be done:

- Legislative authorization should be required before any new technology is deployed that would potentially infringe on civil liberties.
- New technologies should be “neutral”—that is, they should “build in” existing legal and policy limitations on access to individually identifiable information or third-party data and not be seen as a reason to alter existing legal regimes.

- New technologies should be used in a manner that ensures accountability of the executive branch to the legislative by, for example, requiring authorization by a publicly appointed and accountable official before the implementation or use of a new system.
- New technologies should minimize intrusiveness to the extent practical and consistent with achieving counter-terrorism objectives. Depending upon the context, this principle might mean:
  - Ensuring that entry of individual information into the system is voluntary;
  - Whether information entry is voluntary or involuntary, requiring that the use of any new system should be overt, rather than covert;
  - Using information technologies for the verification of information rather than as an independent source of identification;
  - Accessing information already in the possession of the government (which is more readily accepted than is access to information in the private domain);
  - Maintaining data and information in a distributed architecture as opposed to a centralized system in which a big central database is under government control;
  - When possible, making individually identifiable information anonymous (or rendered pseudonymous) and disaggregated so that individual activity is not routinely scrutinized; and
  - Further enhancing protection of individual anonymity by ensuring that individual identities are not tied to information about activities (such as purchases) without the approval of a neutral third-party decision maker (such as a federal judge).
- The consequence of identification by a new technology should not be presumptive. (Such identification is cause for additional investigation, not punitive government action.).
- Any new technology should have strong technological audit and oversight mechanisms to prevent against abuse built into it.
- There should be a robust legal mechanism for the correction of mistakes.

- There should be heightened accountability and oversight, including internal policy controls and training, executive branch administrative oversight, enhanced congressional oversight, and civil and criminal penalties for abuse.
- Finally, any new technology should be deployed with a recognition that many balances struck in the counter-terrorism context would be struck differently in the context of traditional law enforcement. To guard against “mission creep,” we should be especially wary of the instinct to use new enabling technologies in non-terrorism contexts, such as chasing down deadbeat dads.

## The Need for Preventive Detention

One of the most glaring shortfalls in the American response to the terrorist attacks of 9/11 is that we have not yet undertaken the difficult task of defining a legal regime in which actionable intelligence may, in fact, be acted upon. The hearings of the 9/11 Commission have, despite their sometimes rancorous tenor, made one thing clear: Prior to September 11, there were systematic problems that prevented appropriate coordination among various intelligence agencies and between the intelligence community and law enforcement.<sup>22</sup> Fixing that problem is a long and difficult task.

The simple fact is that a lot of good intelligence information has no place in a court of law. As those who are involved in intelligence collection know, much intelligence information, even the best and most accurate information that is directly actionable, is not suitable for use in our existing legal system. Consider:

- Highly accurate information may have been provided by a foreign government, but only on the condition that the information never be publicly disclosed, or indeed, that the fact of the government’s cooperation with us never be disclosed. Using this information, even in the controlled setting of a criminal trial governed by the procedures of the Classified Information Procedures Act (CIPA),<sup>23</sup> would dry up the source of information for all future events.
- Information of unquestioned veracity may have been gathered through sources and methods that are not known to the public or to foreign powers and terrorists. Public disclosure that the

information is in the possession of the United States would compromise the source or method and render it useless.<sup>24</sup> There is some anecdotal evidence that this has already occurred. During the first World Trade Center bombing trial, the government disclosed that it had the capacity to intercept Osama bin Laden's satellite phone calls. It is reported that, naturally, he stopped using satellite phones.<sup>25</sup>

- Rules requiring disclosure of evidence can conflict with national security needs. One need only look at the difficulties created by the trial of Zacarias Moussaoui (the so-called twentieth hijacker) to recognize this problem. Criminal trial rules require that he have access to al-Qaeda operatives (reported to be Khalid Sheik Muhammad and Ramsi Binalshibh) as potential witnesses with allegedly favorable evidence. Yet allowing Moussaoui (or his lawyers) access to Muhammad and Binalshibh while they are still being interrogated would be a foolhardy compromise of vital intelligence assets.<sup>26</sup>
- The rules of evidence in a court of law strictly limit the admissibility of various bits of information. Documents and photographs must be authenticated. Hearsay is not allowed.<sup>27</sup> Yet often the best, most useful, intelligence information cannot meet these legal requirements. A stolen document (or one intercepted by electronic means) often cannot be authenticated. The individual who surreptitiously took a photograph may not be available in an American court to authenticate it. Sometimes the best oral intelligence ("At a meeting last week, Osama said ...") is rank hearsay.
- Finally, one must confront the new reality posed by the "problem" of interrogation. Virtually every practitioner of interrogation will tell you that one of the most successful means of productive interrogation is isolation. As the courts have said, interruption of the interrogation process may "have devastating effects on the ability to gather information" from those who have been captured.<sup>28</sup> Of course, the inability to gather information of this sort could well result in the failure to prevent future terrorist attacks. However, isolation of a terrorist suspect—that is, the denial of access to him by anyone—is inconsistent with existing practices, including rules relating to the provision of counsel.

These are but a few examples of the ways in which the intelligence-gathering function does not mesh with our conception of law enforcement and the legal

system. Of course, not all intelligence information is as substantial as that required in the legal system. Certain intelligence may be enough to raise substantial suspicion, but it may fall far short of information that would establish someone's terrorist intents in a forum requiring proof beyond a reasonable doubt.

Thus the question: What do we do? If, indeed, our law enforcement and intelligence agencies have solid, actionable intelligence of a terrorist threat, and if that intelligence is sufficient to allow the identification of an individual or group of individuals, what should be our response? Under the existing legal system, as we have noted, it may be impossible to arrest suspected terrorists without unacceptable risks and costs. Yet detention outside the existing legal structures is also unacceptable. What then?

## After 9/11

Our lack of a coherent answer to this question explains some of the most problematic and controversial actions taken by our government after September 11. The use of material witness warrants, the wholesale roundup of Arab immigrants in the aftermath of 9/11, and the detention of "enemy combatants" are all responses to this problem. On the merits, these policies have plausible legal grounds. They have engendered much controversy.

Our concern here is not, however, with their legal justification. Rather, it is that, examined objectively, the responses reflect a simple fact: We lack a legal system prepared for dealing with actionable intelligence. In other words, we lack a regularized process for preventive detention in lieu of criminal trial. As one observer has put it (albeit in a different context): "America was put off balance by September 11."<sup>29</sup> What we are doing now is trying to accommodate existing legal procedures to a new reality—in effect, squeezing a square peg into a round hole.

## Material Witness Warrants

One of the first legal responses to the problem of actionable intelligence without a satisfactory legal structure was the use of material witness warrants.<sup>30</sup> Material witness warrants traditionally functioned exactly as their name implies—they were used to arrest and detain witnesses to criminal events when it was anticipated that the witnesses would flee the jurisdiction to avoid the obligation of giving testimony. Immediately after 9/11, a number of individuals

suspected of involvement in terrorist activities were detained through the use of material witness warrants. Some detainees fit the traditional model (at least in part) because they were held pending their testimony before a grand jury. But the traditional rules were broken when the detention of some witnesses continued for a time despite their willingness to give testimony and have it preserved. It was further broken, to the extent that it was a constraint, when one material witness (Jose Padilla) initially held on a material witness warrant, was remanded to military custody as an “enemy combatant.” The material witness provisions became, in effect, a proxy for a preventive detention program.

Challenges to this practice were swift in coming. Those opposing the use of material witness warrants in this manner challenged their use in pretrial investigations. Although the law had historically approved the use of material witness warrants for grand juries,<sup>31</sup> at least one court initially held that the post-9/11 jailing of witnesses pending investigation was a constitutional violation.<sup>32</sup> Eventually, however, the courts held that the material witness statute was applicable to pre-trial investigations, and that the government could lawfully detain a witness, notwithstanding the witness’s willingness to have his or her testimony preserved, provided that the grounds for detention were subject to judicial review under the standard bail statutes.<sup>33</sup>

However, the approval of material witness warrants as a legal tool cannot obscure the practical reality that they were being used for a purpose different from that which Congress initially intended—the detention of witnesses despite the lack of any real need for their testimony. Because this legal structure is not designed to adjudicate issues for the long-term detention of suspected terrorists (rather than the short-term detention of potential witnesses), it lacks any number of legal checks on the exercise of executive authority. The burden of proof placed upon the government to justify its detention is ill-defined. There is only a limited opportunity for those detained to challenge their detention and secure the assistance of counsel. Additionally, because the use of material witness warrants occurs at the interstices of law and intelligence gathering, there is little, if any, sustained congressional oversight of the use of the power.

## “Hold Until Cleared”

Immediately after 9/11, the FBI rounded up a number of Arab immigrants and detained them. In reviewing these detentions, the Inspector General of the Department of Justice concluded that approximately 762 aliens were

arrested. The vast majority of those arrested were detained pursuant to civil immigration law for remaining in the United States after expiration of their entry visas or for entering the country illegally.<sup>34</sup> Despite the relatively unimportant nature of their wrongdoing, each of the detainees was held in the United States until such time as he or she was “cleared” by the FBI of any suspicion of terrorist connections.<sup>35</sup>

The Inspector General did not criticize this policy.<sup>36</sup> Moreover, he acknowledged that in all but one instance the detainees arrested were held on valid immigration charges.<sup>37</sup> It nonetheless remains the case that the implementation of the “hold until cleared” policy was overly inclusive and resulted far more in identifying immigration violations than it did in identifying individuals connected with terrorism.

Given the extremity of the times in which these detentions occurred (most arrests were in New York City or surrounding areas within three months of the attack), the reaction of government authorities was understandable. With the World Trade Center smoldering in lower Manhattan, a robust response was to be expected. In the end, however, immigration law served as a substitute for terrorist detentions—a substitution made necessary by the absence of any other viable legal mechanism.

## Enemy Combatants

Many of the same observations can be made regarding the far more notorious cases involving the detention of Yasser Hamdi and Jose Padilla as “enemy combatants.” Hamdi and Padilla were both American citizens, one caught on the field of battle in Afghanistan and the other detained as he entered the United States at Chicago’s O’Hare airport. The government designated them as enemy combatants subject to special detention rules. These included, at least initially, a prohibition on contact with counsel and a contention that the detention decision was subject to limited judicial review.

Once again, the government’s conduct was a response to a heartfelt perceived need. Although we should not take all of the government’s concerns at unquestioned face value, there is certainly ample basis for thinking that the perception of the need was justified. Padilla, for example, may have planned significant terrorist activities in the United States.<sup>38</sup> Yet it is by no means clear that at the time of his initial detention Padilla could have been criminally charged, or that if charged, he would have been convicted. Thus the problem

recurs again about how to treat those whom credible evidence suggests are engaged in terrorist activities, but for whom the legal system was not designed.

The Supreme Court has now concluded that detentions must be subject to more rigorous review than that initially afforded the detainees.<sup>39</sup> In doing so, the Court recognized that the capture and detention of those who would wage war against the United States was a universal historical practice. However, the Court recognized that the “war” in which we are currently engaged has unusual characteristics—not the least of which is that some aspects of the war have no foreseeable termination. In recognition of this, the Court determined that the Constitution required some form of process for reviewing detention claims, including notice of the factual basis for detention and an opportunity to rebut the factual assertion before a neutral decision maker. The Court left for another day more detailed questions about precisely what form this process would take, including questions about the admissibility of evidence, the burden of proof, and the identity of the decision maker.<sup>40</sup>

The Court’s decision makes the case for congressional action in this area. The question remains: Exactly what sort of process ought to be provided?

What is needed is a new legal architecture to govern the detention of suspected terrorists. Any such system must provide a legitimate process by which we can decide whether those suspected of terrorism are really threats and a means of ensuring that the process is used appropriately—not abused. The challenge is an exceedingly difficult one—one that perhaps admits of no ideal solution. Yet the absence of any legal structure in current law has led to an unsatisfactory *ad hoc* approach. It is a near certainty that the detention powers we propose are a practical necessity. It is equally certain that the exercise of those powers is better constrained—and civil liberties better protected—when the exercise is regularized under the rule of law. Indeed, in the absence of any thoughtful effort to construct such a legal system *before* another terrorist attack on American soil, it is all too likely that the reaction will be similar. There is a need for a better answer.

## An All-American Response

Plainly America needs a more thoughtful, comprehensive legal response to terrorism. It must “regain [its] balance”<sup>41</sup> and adopt a system of laws that truly regulate and constrain executive behavior, while simultaneously allowing the executive to respond effectively in those very narrow circumstances in

which a response is necessary but the existing legal structures are inadequate. Here we outline what such new legal system might look like.<sup>42</sup>

First, the regime of preventive detention that we envision should be limited to cases of terrorism. This requires a narrow definition of terrorism—narrower than that used in current law. Detention will be appropriate only in situations involving individuals who:

- act or threaten to act in a manner that involves serious violence against a person or property and/or in a manner that risks the health and safety of the public; *and*
- does so to influence government policy or intimidate the public; *and*
- does so for the purpose of advancing a political, religious, or ideological cause.

In other words, the “gate” for the preventive detention system must be very narrow. Additionally:

- There must be a rigorous certification process at the front end. No individual should be subject to detention unless the U.S. Attorney General first certifies as to its necessity. The certification should affirm that credible evidence exists that: (a) the individual to be detained intends to commit a terrorist act; (b) the individual is affiliated with a terrorist organization; and (c) the existing criminal legal justice system cannot be applied to the individual without compromising national security.
- This certification should be subject to review in court. The preferred method of review is in an adversarial process in which the detained individual is represented by counsel. To allow assignment of counsel for proceedings in which classified materials are considered, the government should create a group of pre-cleared defense counsel (perhaps as part of the Federal Public Defender system) available for assignment to the detained individual(s).
- Proceedings to determine whether detention is appropriate, would have the following components (as required by the *Hamdi* decision): (a) Notice to the detainee of the factual basis for detention; (b) An opportunity to rebut the detention evidence; (c) A neutral decision maker. To regularize the process and insulate it

from executive influence, we would recommend the creation of a new adjudicative court like the Foreign Intelligence Surveillance Court; (d) Evidentiary rules would be relaxed with modified procedures to account for the need to use classified information, and rules would allow the presentation of evidence *in camera* (or in a form different from that in a traditional criminal trial); and (e) The government would bear the burden of proving the grounds for its detention decision by proof that meets the “clear and convincing evidence” standard—a standard more stringent than that currently used for pretrial detention in criminal cases.<sup>43</sup>

- In rare circumstances the government may have grounds for wishing to delay the detainee’s appearance in court and access to counsel, so that ongoing interrogation can continue. The initial period of delay should be no more than 30 days and any extension of that time period should be periodically reviewed and justified (to the court) by a clear and convincing showing that a further delay is likely to provide additional intelligence.
- To ensure that the preventive detention authority is not abused, there should be routine, systematic oversight. Review of the general process should, of course, reside with the congressional intelligence committees. Beyond that, each individual detention decision should be independently reviewed and the subject of a public report. Possible entities for conducting the review might include the President’s Intelligence Oversight Board or the Inspector General of the CIA.

In calling for Congress to enact legislation concerning this matter, we are not alone,<sup>44</sup> although there are some who will disagree with making the effort at all, who will say that Americans should never allow preventive detention in any form because it is an unwarranted threat to liberty.

The response to this criticism is threefold: First, it ignores reality. We already have incomplete and irregular forms of preventive detention. We advance liberty when we regularize the practice, cabin it to narrow circumstances, and use it sparingly. Second, other countries (such as the United Kingdom) have managed to adopt very limited forms of preventive detention without becoming noticeably “unfree” or “authoritarian.” Adoption of similar legal forms in the United States will not render us an authoritarian regime either.

Finally, and most important, to reject preventive detention in those rare circumstances in which it is necessary is to exalt liberty at the expense of security.

The founding of the American republic was for the purpose of constructing a political system of ordered liberty. It simply cannot be right to unilaterally prefer liberty. Liberty is not an absolute value; it depends upon security (both personal and national) for its exercise. The growth in danger from the consequences of the failure to stop terrorism necessitates altering our tolerance for governmental order. More fundamentally, our goal should be to balance order and liberty.

We achieve order and liberty best, not by closing our eyes to the necessity of security nor by allowing security concerns to run rampant without oversight, but rather by taking appropriate steps to ensure that the powers given to the executive branch are exercised thoughtfully, with care, and subject to continual review and oversight by both the judiciary and the legislative branch. This concept of checks and balances was the fundamental insight of the framers of the Constitution—and is as applicable today as it was at the time of the founding.

## Looking Over Our Shoulders

Perhaps the most important tool we need to develop for securing the future is our own vigilance. To allow us to guard against the abuse of power will require, among other things, knowledge of how that power is being exercised. That requires transparency in the acts of governance. After all, transparency is a vital aspect of democracy. Many of the powers that we need to provide the executive would be unacceptable if their implementation were conducted in secret. As James Madison wisely observed, democracy without information is “but prologue to a farce or a tragedy.” Hoover’s FBI was the embodiment of Madison’s maxim. Unchecked by oversight from Congress, courts, or the public, abuses of public power continued unabated.

Yet transparency is not an absolute value. After all, Madison and others found it necessary to draft the Constitution in a convention whose proceedings were kept secret. Transparency, however, is necessary for oversight: It enables us to limit the executive exercise of authority. It also allows us to empower the executive. If we enhance transparency appropriately, we can also comfortably expand governmental authority, confident that our review of the use of that authority can prevent abuse.

In the post-9/11 world, the form of new oversight should vary depending upon the extent to which transparency and opacity are necessary to the new executive power. Legislation which exempts information supplied by businesses regarding potential terrorist attack risks from public disclosure

offers a case in point. To be sure, there is a potential for abuse of that exemption: Businesses may over-disclose to the government as a means of concealing their operations from legitimate scrutiny by public interest groups. Yet surely, supplying this information to the government is vital to assure the protection of critical infrastructure. Disclosing such information is dangerous, as it risks use by terrorists. Thus, complete transparency will defeat the purpose of disclosure, while complete opacity permits misuse.

What is required is a concept of *calibrated transparency*, a measured, flexible, adaptable transparency suited to the needs of oversight without frustrating the legitimate interests in limiting disclosure. Calibrated transparency can take many forms. These might include enhanced judicial review (placing our trust in judges to oversee the executive branch for us). It also might employ legislative oversight as a proxy for public disclosure, having Congress checking to ensure the laws it passed are being implemented in the way it intended. In appropriate circumstances the transparency might be modified to allow review through closed proceedings. These proxy review mechanisms are substitutes for full transparency, and so the presumption should be in favor of full disclosure.

Transparency is actually enhanced if we recognize that it is not an absolute. In the scenario of infrastructure information, for example, one can readily conceive of calibrated transparency mechanisms (for example, random administrative and legislative auditing) that will guard against abuse, while acknowledging the value of limited disclosure. In short, Madison was not a hypocrite. Rather, opacity and transparency each have a place, in different measures dictated by circumstance. The wisdom of Madison's insight—that both are necessary—remains as true today as it was 220 years ago.

Therefore, as we proceed in providing additional authorities to the government as a means of combating terrorism, we must do so in a way that allows for oversight of the right forms. In some instances, this means a reformed and reinvigorated congressional oversight system. In others, it is judicial oversight. In still others, there must be public disclosure and debate.

## Past Time for the Next Steps

When the Cold War began, it was more than ten years before the legal and structural systems that would sustain us through the fifty-year struggle were put in place. Even then, men like Hoover found ways to circumvent the rules when it served their purposes.



Screening passengers at the airport in Fargo, North Dakota after 9/11. (PHOTO BY NOBLE EAGLE MASTER SERGEANT WILLIAM J. QUINN COURTESY OF THE U.S. AIR FORCE/NORTH DAKOTA AIR NATIONAL GUARD)

We should get started now. We cannot, and should not, expect that at the start of this long struggle we will get it right the first time. 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 forebears and the experience of our own time.<sup>46</sup>

Others have echoed that call.

The debate will continue. The courts and Congress are well positioned to fix any problem with additional legislation or more decisions interpreting the laws.

That is exactly as it should be. 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.”<sup>47</sup>

Thus, the obligation of the government is a dual one: to protect civil safety and security against violence *and* to preserve civil liberty. Viet Dinh used almost the exact same argument to describe the government’s role in fighting the war on terrorism: “The function of government is the security of its polity and the safety of its people. For without them there will be no structure so that liberty can survive. We see our work not as a balancing security and liberty,” Dinh declared, “rather, we see it as securing liberty by assuring the conditions of true liberty.” We can achieve that goal, but there is more work to done.