

# 4 The USA Patriot Act

## A Challenge to Equal Justice?

[A] man has property in his opinions and the free communication of them. He has a property of peculiar value in his religious opinions, and in the profession and practices dictated by them. He has property very dear to him in the safety and liberty of his person. He has an equal property in the free use of his faculties and free choice of the objects on which to employ them. In a word, as a man is said to have a right to his property, he may be equally said to have a property in his rights.

—James Madison, *Essay on Property*, 1792

The true danger is when liberty is nibbled away, for expedients, and by parts. . . . the only thing necessary for evil to triumph is for good men to do nothing.

—Edmund Burke

A quarter-century ago, the Senate Select Committee to Study Governmental Operations issued its final report with respect to intelligence activities within the United States. Named after its chairman, Senator Frank Church, the Church Committee was charged with conducting a wide-ranging investigation into governmental intelligence activities in the wake of the Watergate scandal. To effectuate this mandate, the committee interviewed hundreds of individuals and pored through voluminous documents generated by the FBI, CIA, NSA, and IRS, as well as many other federal agencies with intelligence-gathering responsibilities. In its painstakingly detailed final report, the committee found, among other things, that

domestic intelligence activity has been overbroad in that (1) many Americans and domestic groups have been subjected to investigation who were not suspected of criminal activity and (2) the intelligence agencies have regularly collected information about personal and political activities irrelevant to any legitimate government interest.<sup>1</sup>

The committee further determined that although the government had a responsibility to act in the face of legitimate national security concerns, including intelligence efforts by Nazi Germany, Japan, and the Soviet Union,

appropriate restraints, controls, and prohibitions on intelligence collection were not devised; distinctions between legitimate targets of investigations and innocent citizens were forgotten; and the Government's actions were never examined for their effects on the constitutional rights of Americans, either when programs originated or as they continued over the years.<sup>2</sup>

Typical of these investigative techniques, for example, was an Army Domestic Surveillance program developed in the late 1960s, which permitted the armed forces to collect information on and scrutinize the behavior of "dissidents," "instigators," "group participants," and "subversive elements." Later, these already vague criteria were broadened even further to include "prominent persons who were friendly with the leaders of the disturbance or sympathetic with their plans." In a vain attempt to add some semblance of specificity, the program suggested that likely targets for rooting out such dissidents might include the "civil rights movement" and the "anti-Vietnam/anti-draft movements," two very prominent political factions of the 1960s.<sup>3</sup>

Applying these nebulous standards, the Army created intelligence files on nearly 100,000 innocent American citizens, including clergymen, attorneys, authors, athletes, and business executives whose "crime" was nothing more than their constitutionally protected participation in political protests or association with those who engaged in such activities. The Church Committee concluded that this wholly unjustified intrusion into the lives of Americans was a direct result of the inexplicable and unpardonable failure of

the legislative branch to “enact statutes precisely delineating the authority of the intelligence agencies or defining the purpose and scope of domestic intelligence activity.”<sup>4</sup>

As if time stood still and the lessons of history were fleeting, the recently enacted Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, best known by its acronym, the “USA Patriot Act,” offers yet another glimpse of an America tragically surrendering her democratic principles to the whims of contemporary fears and prejudices. At this writing, America is approaching the second anniversary of a terrorist attack so unimaginable that even two years later the images remain as incomprehensible as the day they were first broadcast to a disbelieving national audience. Over time, disbelief turned to dismay, which eventually gave way to passionate demands that the government act promptly to avenge the senseless tragedy. A mere six weeks after the attacks, with the nation still struggling amid overwhelming emotional and political turmoil, the USA Patriot Act was signed into law by President George W. Bush, ostensibly signaling to the global community that although America’s resolve had been severely tested she was nevertheless ready to meet the challenges ahead.

Reviewing its brief history in Congress, the Patriot Act originated in the House of Representatives as H.R. 2975 (the Patriot Act) and in the Senate as S.1510 (the USA Act). The House subsequently passed H.R. 3162 (under suspension of rules), which resolved critical differences between 2975 and 1510. The resulting 342-page legislative tome, which amends more than fifteen different statutes and grants sweeping new powers to law enforcement and intelligence officials to combat terrorism at home and abroad, then passed by overwhelming margins in both the Senate—98–1—and the House of Representatives—356–66. In an unprecedented abrogation of long-standing legislative process, prior to its passage the Patriot Act was not carefully analyzed, studied, or debated; no testimony from experts or impacted parties was solicited or heard; and no conference or committee reports were issued. In short, the normal legislative vetting process was almost completely abandoned in an attempt to fast-track the legislation to passage. Not surprisingly, the process (or lack thereof) surrounding passage and the substance of

the legislation were met with immediate and withering criticism from civil liberties organizations.

Apparently undaunted by the blistering attacks, the Bush administration hailed the legislation as a resounding blow against terrorism, which is not entirely surprising given that many of the more controversial portions of the Patriot Act are based, in part, upon a DOJ counterterrorism “wish list” submitted to Congress little more than a week after the devastating 9/11 attacks. The DOJ memorandum to Congress proposed that appropriate legislation be enacted or amended to bolster the government’s aggressive new counterterrorism initiative. Specifically, the DOJ proposal called upon Congress to authorize:

- the unprecedented sharing of confidential grand jury information with the U.S. intelligence community;
- the weakening of standards for obtaining court authorization for surveillance activities under the Foreign Intelligence Surveillance Act (FISA) by removing the “agent of a foreign power” requirement;
- the restoration of presidential power to confiscate and vest in the U.S. property of enemies during times of national emergency;
- the broadening of the definition of terrorist to include “anyone who affords material support to an organization that the individual knows or should know is a terrorist organization, regardless of whether or not the purported purpose for the support is related to terrorism”;
- the attorney general’s office to detain those illegally in the United States who, as determined by the attorney general, pose a threat to national security, whether or not the alien is eligible for or is granted relief from removal from the United States;
- the removal of any statute of limitations for “terrorism offenses” committed before or after the effective date of the statute; and
- the institution of lengthier periods of postsupervision release for persons convicted of a crime, including the possibility of lifetime tracking and terrorist oversight.<sup>5</sup>

Although the Patriot Act as enacted did not incorporate all of the modifications proposed by the DOJ, the list is a compelling reminder of the hard-line, constitutionally questionable stance espoused by an administration seemingly ignorant of the historical reminders that excess in times of national upheaval is a recipe for disaster.

As enacted, the USA Patriot Act consists of ten separate titles, each containing a multitude of sections. Substantively, the act enhances many existing crimes, creates new crimes, extends statutes of limitation, toughens penalties, and grants unparalleled power to the executive branch, with correspondingly minimal judicial or congressional oversight. Perhaps most importantly, in the rush to passage, Congress failed to critically evaluate whether these statutory tools are even necessary to fight the so-called war on terrorism, apparently either ignoring their fact-finding authority or ceding it to the executive branch. However, assuming such a legislative overhaul is essential to the antiterrorism agenda, then Congress also neglected its constitutional responsibility to oversee and limit, if necessary, the executive's power to abuse its new authority, a startling yet patent indication of excessive deference to the executive branch.

Indeed, in an apparent acknowledgment of these failings, on October 25, 2001, during a debate session that leaned more toward the appearance of procedural propriety than substantive analysis, Senator Patrick Leahy conceded that such a weighty piece of legislation required meaningful congressional debate and discussion but insisted that "there is no question that we will vote on this piece of legislation today and we will pass this legislation today." Moreover, recognizing that the haste with which the bill was produced might result in questionable legislation, Leahy delivered an ominous prediction: "I do believe that some of the provisions contained . . . in this bill . . . will face difficult tests in the courts, and that we in Congress may have to revisit these issues at some time in the future when the present crisis has passed, the sunset has expired or the courts find an infirmity in these provisions."<sup>6</sup>

Interestingly, Leahy's determination to upend legislative process in favor of swift resolution was in sharp contrast to his demeanor during the glaringly superficial debate on another piece of coun-

terterrorism legislation, the Combating Terrorism Act (CTA). The CTA was proposed just two days after the 9/11 events and was subsequently passed by the Senate in the middle of the night on the same day it was submitted.<sup>7</sup> Leahy scathingly criticized the Senate's haste to enact the CTA, offering the following observations:

Somewhere we ought to ask ourselves: do we totally ignore the normal ways of doing business in the Senate? If we do that, what is going to happen when we get down to the really difficult questions? Maybe the Senate wants to just go ahead and adopt new abilities to wiretap our citizens. Maybe they want to adopt new abilities to go into people's computers. Maybe that will make us feel safer. Maybe. And maybe what the terrorists have done made us a little bit less safe. Maybe they have increased big brother in this country. If that is what the Senate wants, we can vote for it. But do we really show respect to the American people by slapping something together, something that nobody on the floor can explain?<sup>8</sup>

Despite Leahy's adamant remarks concerning adherence to process and legislative precision during the Senate's consideration of the CTA, Senator Jon Kyl's passion-filled comments echoed the raw sentiments of the majority of those present and ultimately carried the day:

Let me be very clear about the intent of this legislation. This country has just suffered the worst terrorist attack in its history. All of us are focused on the victims. We are focused on the terrible devastation and the individual lives impacted. But, as policymakers, we have also been asked some hard questions by our constituents and those questions include things such as: Why can't our Government do something about these horrible crimes? As policymakers, we have to respond to that. Our constituents are calling this a war on terrorism. In wars, you don't fight by the Marquis of Queensberry rules. The time to be overly punctilious about who you get to work with you to get information from the enemy ought to come to an end.<sup>9</sup>

## The Road to Equal Justice: A Brief Historical Reflection

### EQUAL JUSTICE in the balance

120

Assuming *arguendo* that, as Senator Kyl urges, Americans are pleading with the government to “do something” about the horrific events of 9/11, can such a demand be taken to blithely cede authority to the government to disregard constitutional values in pursuit of vengeance? As British statesman and political philosopher Edmund Burke observed two centuries ago, a free people “augur misgovernment at a distance; and snuff the approach of tyranny in every tainted breeze.”<sup>10</sup> Consequently, if history is indeed an accurate indicator, then the call for governmental action in the wake of 9/11 is not intended as *carte blanche* authorization to annihilate the constitutional underpinnings of America’s democratic society.

At its inception, America was a relatively free country with a zealous adherence to the social compact theory. This philosophy, grounded in the predominant political thinking of the times, mandated that every citizen in the prepolitical state possessed God-given or natural rights, and the constitutional system of government originated as a consensual mechanism designed to protect and ensure those natural rights. This limited conferral of power meant that government existed solely by the consent of the governed, which necessarily implied that governmental authority could be constrained so as not to impinge upon natural rights and individual liberties.

To memorialize these tenets and appropriately define governmental powers and constraints, the Founding Fathers reasoned that the basic charter for the new government must incorporate standardized procedures known and applicable to all so as to avoid arbitrary and capricious governmental behavior. Precolonial experiences in England taught the drafters that “[v]icious and ad hoc procedures . . . [could be] used to victimize religious and political minorities [and] . . . [o]ne’s home could not be his castle or his property be his own, nor could his right to express his opinion or to worship his God be secure, if he could be searched, arrested, tried, and imprisoned in some arbitrary way.”<sup>11</sup>

The Bill of Rights evolved as the vehicle to simultaneously preserve these natural rights and impose limitations on governmental power. Originally omitted from the Constitution, the Bill of Rights added ten substantive amendments to the Constitution and became

the unlikely basis for ratification compromise after a relatively short but contentious political struggle. Ultimately, its inclusion in America's founding charter represented a triumph of individual liberty against government power, which is, as Leonard Levy points out, "one of [American] history's noblest themes."<sup>12</sup>

Over time, the Fourth Amendment emerged as the chief constitutional means for preserving personal liberties and restraining the unreasonable exercise of governmental power in the criminal justice context. Although notably brief—a mere fifty-four words—the amendment articulates the fledgling nation's abhorrence for arbitrary and capricious governmental intrusion into specific zones of personal privacy. As ratified, the Fourth Amendment states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Prior to the ratification of the Fourth Amendment, early settlers in America, newly freed from an oppressive English monarchy, professed a fierce belief in the "home is castle" ideology. However, the laws and corresponding actions of government officials in the new world were the antithesis of these sentiments. As Levy describes, in colonial America a man's home was hardly his castle, and general searches, which were commonplace occurrences in England, became the norm on the American continent. To facilitate these intrusions, magistrates issued warrants based upon mere suspicion, as the modern notion of probable cause was nonexistent. Use of such illimitable search and seizure practices continued during the Revolutionary War, when they were primarily implemented to banish those of questionable loyalty or those who refused to take an oath of allegiance to the country. Having thus experienced the scourge of unchecked governmental search and seizure authority, postrevolutionary America was eager to institute governmental systems that effectively reined in law enforcement excess while still permitting searches to be utilized as a tool in the crime-fighting arsenal.

One of the earliest reported cases challenging the legality of the

general warrant was *Frisbie v. Butler*.<sup>13</sup> In that case, the complainant, one Josiah Butler, suddenly discovered missing “twenty pounds of good pork” and suspected the defendant, Benjamin Frisbie, of stealing the cache. Butler made application to the local magistrate for a general warrant to search for meat. The warrant, directed to the appropriate authority, was issued with the following language:

By authority of the state of Connecticut, you are commanded forthwith to search *all* suspected places and persons that the complainant thinks proper, to find his lost pork, and to cause the same, and the person with whom it shall be found, or suspected to have taken the same, and have him to appear before some proper authority, to be examined according to law.<sup>14</sup>

Upon conviction, Frisbie appealed, arguing, among other things, that his arrest was effected pursuant to a general search warrant, commanding *all persons and places* throughout the world to be searched, at the discretion of the complainant. The warrant’s unnecessarily broad parameters, Frisbie contended, were illegal and, therefore, void. The court, in its opinion, concluded that, because the warrant imposed no limitations on its execution and authorized officers to search all places and arrest all persons whom the complainant should suspect of purloining the pork, it was patently illegal. In a further attempt to provide future guidance to issuing authorities, the court observed that “it is the duty of a justice of the peace granting a search warrant (in doing which he acts judicially) to limit the search to such particular place or places, as he, from the circumstances, shall judge there is reason to suspect; and the arrest to such person or persons as the goods shall be found with.”<sup>15</sup>

The Frisbie case and others of its ilk sowed the seeds for a constitutional amendment that solemnized the sentiments expressed in the Frisbie court’s opinion. Yet, according to Levy, the Fourth Amendment was no panacea. While it articulated specific areas of privacy immune from unreasonable government intrusion and represented a swift and decisive liberalization of the law of search and seizure, it provided no remedy for violations of its dictates and introduced vague concepts such as “probable cause,” which ultimately became the determinative factor for deciding whether a search or seizure was constitutionally reasonable.

Yet another avenue for governmental intrusion exists because the core foundation upon which the Fourth Amendment rests—the right to privacy—finds no express support within the four corners of the Constitution. That is, although Fourth Amendment protections are constitutionally grounded in “reasonable expectations of privacy,” the framers did not explicitly articulate such a right, much less define its parameters. Instead, the U.S. Supreme Court later recognized that the right to privacy emerges from the “penumbras” of specific guarantees of the Bill of Rights. Expounding on this right to privacy, the Court, in the ground-breaking case of *Griswold v. Connecticut*, observed:

specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment in its prohibition against the quartering of soldiers “in any house” in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the “right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: “The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.”<sup>16</sup>

Speaking more specifically to Fourth Amendment protections, the Court noted that, where innocent citizens are concerned, it is not the breaking of doors or the rummaging through of drawers that constitute the essence of a Fourth Amendment violation, for these are minor annoyances. Instead, the injury arises from the invasion of the “indefeasible right of personal security, personal liberty and private property, where that right has never been forfeited by . . . conviction of some public offence.”<sup>17</sup> These are the very rights that are in grave jeopardy of perishing under the weight and breadth of the USA Patriot Act.

## Expanded Surveillance Authority and Threats to Privacy

**EQUAL JUSTICE**  
in the balance

124

The USA Patriot Act increases governmental authorization for practically every surveillance apparatus currently available to the government. To date, these tools consist of an extensive variety of mechanical, digital, and legal devices, including wiretaps, pen registers, trap and trace devices, the Carnivore system, subpoenas, and search warrants. In conjunction with this newly expanded authority, the Patriot Act also broadens the definition of terrorism, thereby exponentially increasing the possibility of surveilling more categories of people with these myriad investigative instruments. If historical precedent is an important teacher, then unfettered governmental authority to spy on its citizens can be quickly transformed into an absolute license to invade the privacy of innocent individuals (especially disfavored groups) in the name of national security.

Early in the twentieth century, legislation circumscribing the government's domestic clandestine investigative techniques became necessary as the feasibility of surreptitiously capturing private conversations expanded with the inventions of the microphone, telephone, and dictograph recorder. Initial court challenges to evidence obtained through such covert means were largely unsuccessful, however, as the U.S. Supreme Court interpreted the Fourth Amendment to narrowly protect property rights from unwarranted *physical* trespass into protected places. Thus, as long as the recording device could be placed without physically invading private areas, then the Fourth Amendment was inapplicable. The Court also strictly defined property as tangible assets, thus barring the inclusion of mere "information" obtained by eavesdropping. Later, in a series of opinions, the Court reversed direction and dispensed with both unpersuasive rationales for supporting such unwarranted governmental intrusions, observing in *Katz v. United States* that

[o]ver and again this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes . . . and that searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject

only to a few specifically established and well-delineated exceptions.<sup>18</sup>

According to the Court, “bypassing a neutral predetermination of the scope of a search leaves individuals secure from Fourth Amendment violations only in the discretion of the police.”<sup>19</sup> The Court, however, left open the possibility that safeguards other than review by a neutral magistrate might be constitutionally permissible in situations involving national security, thereby laying the groundwork for a secret court system dedicated to authorizing surveillance when national security issues are implicated.

Accepting the Court’s implicit invitation in *Katz* and its progeny to craft a federal statute delineating government surveillance practices, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968, a far-reaching piece of legislation authorizing the procurement of warrants for electronic surveillance but imposing strict judicial oversight throughout the process.<sup>20</sup> Title III provides, for example, that the attorney general or other specifically designated officials may apply for wire or oral interception for certain enumerated felonies.<sup>21</sup> To limit the possibility of arbitrary determinations based on vague and shifting criteria, Title III applications must be in writing and describe with particularity the alleged criminal offense and the location and place of the proposed electronic interception. Moreover, because Title III electronic surveillance is considered a “last resort” investigative technique, the application must discuss specific alternatives to interception and explain why those options are not equally practicable under the circumstances. Finally, the application must identify the proposed time frame for the interception in light of the circumstances of the underlying criminal investigation.

Based upon this information, the court reviewing the Title III application must find probable cause that electronic interception will yield evidence of criminal activity before issuing an order authorizing the surveillance. In that order, the court must carefully instruct law enforcement officials regarding the scope and content of the interception, the type of communications sought, and the duration of the order. Specifically, Title III requires that the order indicate:

- (a) the identity of the person, if known, whose communications are to be intercepted;
- (b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;
- (c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;
- (d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and
- (e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.<sup>22</sup>

Perhaps most importantly, however, when executing the court's order, law enforcement personnel are required to make every effort to limit indiscriminate or arbitrary eavesdropping unrelated to the focus of the investigation to protect the privacy interests of innocent third parties. In practice, of course, this requires agents to listen, at least momentarily, to every conversation transmitted over a particular line to determine its relevance, thereby diminishing the privacy interests of all who converse via that medium, even if only in a *de minimus* fashion.

Title III did not encompass every mode of surveillance technology, and as more sophisticated methods for eavesdropping were developed, Congress dutifully enacted statutes governing the use of those tools in criminal investigations. For example, the pen register, a device that decodes electronic impulses enabling the identification of a telephone number dialed, and trap or trace devices, which decode impulses to discover incoming telephone numbers, are among the surveillance tools requiring judicial authorization prior to implementation. However, because the information obtained by use of these devices is negligible (mere telephone numbers and no conversation content), law enforcement personnel need only demonstrate to the court that the records likely to be obtained by the installation and use of these tools is relevant to an ongoing criminal investigation.

As noted earlier, the U.S. Supreme Court allowed for the possibility that domestic national security investigations directed toward foreign agents or powers might fall outside the parameters of Fourth Amendment protections and, once again, invited Congress to enact standards governing such investigations. Wary of accusations of legislating from the bench, the Court cautioned that, while not attempting to guide congressional judgment in these matters, it was patently obvious that the same type of standards and procedures prescribed by Title III are not necessarily applicable to cases where national security concerns are implicated. Indeed, the Court expressly recognized

that domestic security surveillance may involve different policy and practical considerations from the surveillance of “ordinary crime.” The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in Title III. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government’s preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crime. Given these potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens.<sup>23</sup>

Consistent with the Court’s implicit direction, the executive branch sought legislation establishing a “separate track” for electronic surveillance directed to national security concerns, and Congress acceded to that request by enacting legislation loosening electronic surveillance standards when foreign intelligence matters

were implicated. FISA fashioned guidelines for the collection of foreign intelligence information without regard to whether any criminality was involved. According to the DOD, FISA facilitates the U.S. counterintelligence mission by permitting electronic surveillance, which is critical to detecting espionage, sabotage, terrorism, and related hostile intelligence activities in order to deter, neutralize, or exploit them.

Generally, under FISA, electronic surveillance is permissible if there is probable cause to believe that the target is a foreign agent or foreign power and the “primary purpose” of the investigation is collection of foreign intelligence information. The FISA statute also established a special secret court composed of federal district court judges to review applications for electronic surveillance orders for purposes of foreign intelligence gathering. As will be discussed more completely later in this chapter, until recently, the FISA court operated under a shroud of secrecy, revealing no public information concerning electronic surveillance, with the exception of an annual report detailing the number of requests made and the number granted. The court had never refused a request in its twenty-one-year history until its recent head-on collision with FISA requests arising under the seemingly boundless USA Patriot Act.

Upon obtaining a FISA court order, the government is permitted to use electronic surveillance methods similar to those implemented for domestic purposes, for example, wiretaps, pen registers, and trap or trace devices. Government agents may also make covert physical entries onto premises to acquire foreign intelligence information. Notably, because of the FISA statute’s foreign intelligence orientation and less restrictive guidelines for securing court orders, it draws a distinction between “U.S. persons” and “non-U.S. persons” for purposes of classification as “foreign agents or powers.”<sup>24</sup> Specifically, U.S. persons may not be the target of a FISA order unless there is probable cause to believe that they are acting on behalf of a foreign power and engaged in or about to engage in activities that violate U.S. criminal laws. However, mindful of the potential chilling effect on constitutionally protected behavior, the FISA statute directs that, as it pertains to U.S. persons, activities protected by the First Amendment may not form the sole basis for determining foreign agent status. Finally, FISA authorizes the DOJ to engage in electronic surveillance to collect foreign intelligence

information without a court order for periods of up to one year, with one caveat: There must be no “substantial likelihood” that the intercepted communications include those to which a U.S. person is a party.

As explained, the USA Patriot Act significantly expands the government’s power to utilize a variety of devices to surreptitiously intrude into protected private areas of citizens and noncitizens alike. For example, the implementation of pen register and trap and trace devices is no longer limited to telephone technology. Section 216 of the act now authorizes the use of pen registers and trap and trace devices to capture “dialing, routing, addressing and signaling” information from computer conversations “anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.”<sup>25</sup> The government is, however, prohibited from tracking the *contents* of wire and electronic communications with these devices, and therein lies the critical difference. For while the use of these surveillance tools on traditional telephone technology is fairly noncontroversial because of the minimal amount of information revealed, the expansion of this investigative resource to digital communications, primarily e-mail, is particularly troublesome. Unlike telephonic communications, where such electronic surveillance devices can only capture numbers dialed to or from locations, routing and addressee information encoded in digital exchanges can contain a plethora of additional revelatory information, thus potentially granting the government access to private information that is well beyond the scope of its investigation. Key to the potentially confusing implementation of this section and consequent invasions of privacy is the lack of definitional precision. While the term *content* is clear in the context of telephone communications, the digital landscape does not lend itself to such unambiguous distinctions. For instance, Web site addresses may technically fall within the category of “addressing information,” yet such addresses clearly reveal a wealth of content once accessed, and some Web addresses may even disclose information simply by virtue of their name designations. The potential ability of governmental authorities to track and catalog Web site addresses raises the frightening specter of database warehousing and profiling of targets using com-

posite information that is exponentially more revealing than a mere catalog of telephone numbers dialed or calls received.

The use of the Carnivore system, a controversial computer tracking program capable of capturing *all* communications on any network where it is installed, is also authorized by Section 216. While the government is required to maintain specific records associated with Carnivore's installation and use, such record keeping does little to quell suspicions of governmental overreaching and, ironically, likely increases public apprehension concerning the government's ability to compile private information for purposes of covert profiling.

The Patriot Act also grants the DOJ's request to modify the already lenient standard for implementing pen register and trap and trace devices under FISA. Section 214 now permits the government to obtain orders for electronic surveillance under FISA if sought as part of "any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." Previously, FISA pen register and trap and trace device standards required that the telecommunications device be "used to contact an agent of a foreign power engaged in international terrorism or clandestine intelligence activities." The new powers under this amendment potentially subject American citizens to the vagaries of a secret court system, which, with its Kafkaesque implications, is the absolute antithesis of the U.S. accusatory system of justice. Similar to the expansion under Title III, FISA orders can also now be obtained to capture computer source and addressing information, again with the caveat that such orders cannot be directed against American citizens based solely upon activities protected by the First Amendment.

With respect to stored electronic communications, Section 209 of the act mandates that recorded voice mail messages shall now be treated the same as stored e-mail and communications records held by third parties for purposes of governmental access. That is, law enforcement personnel may obtain a search warrant to access the content of a stored communication, and if the communication has been in remote storage for more than 180 days, the application may

be made and the warrant issued without notice to the subscriber. If probable cause to secure a search warrant is lacking, the government may obtain a court order (with prior notice to the customer or subscriber) “if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.” However, notification to the customer may be delayed for up to ninety days if it is determined that such notice could, among other things, endanger lives, cause the destruction of evidence, seriously jeopardize an investigation, or unduly delay a trial. Another seemingly mundane, but ultimately intrusive, amendment to this section adds credit card and bank account numbers to the list of information that may be demanded from the service provider. The DOJ wish list offered the following explanation for requesting that Congress impose this further requirement:

In fast-moving investigation[s] such as terrorist bombings—in which Internet communications are critical methods of identifying conspirators in determining the source of the attacks—the delay necessitated by the use of court orders can often be important. Obtaining billing and other information can identify not only the perpetrator but also give valuable information about the financial accounts of those responsible and their conspirators.<sup>26</sup>

Section 215 of the act now permits the director of the FBI or his designee to make an application for an order requiring production of tangible things for investigations to protect against terrorism or clandestine intelligence activities. Once again, if the request is directed toward a U.S. citizen, the act mandates that the investigation may not be based solely upon activities protected by the First Amendment. The act also cloaks this surveillance conduct in the utmost secrecy, requiring that the order not disclose that it is issued for purposes of a foreign intelligence investigation. In addition, “[n]o person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section.” The deleterious effect of Section 215

has already been demonstrated. According to a national survey conducted by the University of Illinois at Urbana-Champaign's Library Research Center, law enforcement officials had approached at least eighty-seven libraries for patron records by January 2002, and the actual numbers of requests are believed to be much higher. Many libraries, in turn, have begun purging their patron files every week instead of every couple of months in an effort to protect the privacy of their patrons. Similar "protest" activities by libraries include shredding the computer use sign-up sheets and posting signs warning patrons about the federal government's ability to review their patron records without their knowledge. As Leigh Estabrook, director of the center, observed:

Public libraries are one of the last public spaces in our community and so there's a sense that officials want to get at that public behavior. . . . For me and a number of my colleagues, we are quite worried about the chilling effect to use public libraries and the differential effect on the poor who don't have Internet access except at the public library. We know that librarians are really worried about it, but because of the gag order we don't know how many librarians are cooperating with [requests] and I can't, in good conscience, ask them. I don't think we will know unless someone is successful in a request through the courts.<sup>27</sup>

As to the ultimate impact of this section of the act, Estabrook strikes a decidedly resigned, although cautiously hopeful, tone, concluding, "It's really a judicial issue now." Indeed.

The act also amends the FISA statute in a number of ways that grant the government more authority to exchange information with domestic law enforcement personnel during the course of foreign intelligence investigations. More specifically, Section 218 eliminates the requirement that foreign intelligence gathering be the sole or primary purpose of the investigation and now only requires that it be a "significant purpose." Thus, it is now possible for law enforcement agents to obtain court orders for electronic surveillance and physical searches upon showing "that a significant purpose of the search is to obtain foreign intelligence information." This amendment represents a radical departure from the reasonably bright line

separating domestic criminal investigations and foreign intelligence gathering and has far-reaching implications in terms of its potential to eviscerate due process standards and trample the rights of innocent individuals.

Three decades ago, when the U.S. Supreme Court acknowledged the potential for different investigative standards, and Congress responded by establishing the separate foreign intelligence investigation track under FISA, the apparent basis for permitting more relaxed standards under FISA was the understanding that foreign intelligence gathering operations were not criminal investigations and, therefore, did not require the same judicial oversight. Allowing foreign intelligence investigations to proceed as long as gathering foreign intelligence information is a “significant reason” confers wide latitude on law enforcement officials to conflate criminal investigation purposes among the reasons for obtaining court orders under FISA. Not only does this amendment sanction end runs around traditional Fourth Amendment standards, but it fosters an environment where privacy standards are subject to the whims and creativities of the executive branch, an absolute, although unfortunately not unprecedented, affront to the core principles of democracy. The question that looms large is whether the courts will once again intercede to rescue the Constitution from the current executive stranglehold before history, with all of its tragic consequences, repeats itself.

Complementing the broader authority to obtain court orders under the FISA “significant purpose” standard, Section 203 of the Patriot Act dramatically increases the possibility that information gleaned from unrelated criminal investigations will be shared with the intelligence community. As a launching point to encourage this unbridled exchange of information, the act now permits disclosure of grand jury material “when the matters involve foreign intelligence or counterintelligence . . . or foreign intelligence information . . . to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties.” This sharing of traditionally secret proceedings represents a shocking departure from compelling historical precedent emphasizing and respecting the sanctity of the grand jury process. This development is particularly disturbing because of the

role the grand jury plays in the American criminal justice system. The familiar maxim that “a grand jury would indict a ham sandwich” is indicative (albeit cynically) of the fact that its role is to review the *government’s* evidence and to determine whether an indictment will issue. To aid in its search for the truth, the grand jury has extensive subpoena authority and may compel witnesses to appear and provide testimonial and/or documentary evidence. However, because the government’s evidence is largely unchallenged in most instances, only the flimsiest of cases fail to attain indictment status, and even then the government may convene another grand jury in hopes of achieving a different outcome. It certainly does not require a great leap of imagination to envision the eventual unfettered sharing of one-sided evidence that lacks indicia of criminality but nevertheless subjects targets to continual surveillance and investigatory tactics by various branches of the law enforcement bureaucracy.

Historical justifications for enshrouding grand jury proceedings in secrecy include encouraging witnesses to speak freely and truthfully without fear of negative repercussions and avoiding the unfair stigmatization of targets of criminal probes in the event that an indictment is not issued. Disclosure, even for purposes of aiding national security, defeats each of these justifications and converts the grand jury into a largely unrestricted ancillary investigatory tool in the war on terrorism. The only statutory veneer of protection against rendering grand juries as “witch hunting” venues for foreign intelligence investigations is the requirement that *after* the disclosure the “government shall file under seal a notice with the court stating the fact that such information was disclosed and the departments, agencies, or entities to which the disclosure was made.”

In accordance with the Patriot Act’s implicit goal of conjoining criminal investigations with foreign intelligence gathering, Section 203 also provides that information gathered through electronic means under Title III is subject to disclosure to the extent that the contents pertain to foreign intelligence information.

Yet another addition to the invasive arsenal already at the government’s fingertips arises out of Section 213, which authorizes so-called sneak and peek search warrants. Unlike traditional search warrants, where execution of the warrant generally results in notice, seizure, and the inventory of evidence, sneak and peek war-

rants permit law enforcement officials to enter protected areas, either physically or virtually, to merely search for evidence of a criminal offense without prior notification to owners or other interest holders if the court “finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result.” According to the statute, such adverse results might include the risk of destruction of evidence, bodily injury, and the potential to jeopardize an investigation or to delay a trial proceeding. Thus, while sneak and peek warrants limit the government to conduct that does not physically deprive the owner of property, such intrusive investigation practices can nevertheless facilitate the compilation of an abundance of information concerning a target simply by entering a premises to observe, take measurements or pictures, copy documents, or download computer files.

Section 213 directly contravenes the spirit of Rule 41(d) of the Federal Rules of Criminal Procedure and myriad legal precedents establishing notice of government intrusion into private spaces as a preeminent requirement of the Fourth Amendment. Specifically, the rule stipulates that

the officer taking property under the warrant shall give to the person from whom or from whose premises the property was taken a copy of the warrant and a receipt for the property taken or shall leave the copy and receipt at the place from which the property was taken. The return shall be made promptly and shall be accompanied by a written inventory of any property taken.

As written, the rule imposes no limitations on the nature of “property” and is arguably applicable even if the “property” taken is intangible information, such as in the case of a sneak and peek warrant. Moreover, the U.S. Supreme Court has determined that “we have little doubt that the Framers of the Fourth Amendment thought that the method of an officer’s entry into a dwelling was among the factors to be considered in assessing the reasonableness of a search or seizure . . . [and] in some circumstances an officer’s unannounced entry into a home might be unreasonable under the Fourth Amendment.”<sup>28</sup> In practice, this reasonableness standard

generally means that, barring exigent circumstances, law enforcement personnel desiring entry onto the premises must knock and verbally announce their presence and purpose so as to provide adequate notice to the occupants. Such a requirement protects both officers and citizens because it signals the initiation of a presumptively legal encounter with law enforcement agents and individuals opening their doors with notice of this fact are presumed to submit to that lawful authority. Obviously, reasonableness does not require knock notice when exigent circumstances prevail, such as the likelihood that evidence may be destroyed or when a threat to the officer's safety exists. Overall, the reasonableness of most searches and seizures conducted under the Fourth Amendment appears to be predicated upon timely notice to affected parties.

A further concern arising under this section and premised on Fourth Amendment jurisprudence is, even if covert entry for purposes of mere investigation falls through a loophole in the Constitution, to what extent does the Fourth Amendment nevertheless require timely notification *after* surreptitious entry? In the case of *Dalia v. United States*, the U.S. Supreme Court determined that there was "no basis for a constitutional rule proscribing all covert entries" and made explicit what had long been implicit in their decisions addressing this issue: "The Fourth Amendment does not prohibit per se a covert entry performed for the purpose of installing otherwise legal electronic bugging equipment."<sup>29</sup> Although relevant, the *Dalia* case holding is seemingly limited to circumstances involving covert entries for purposes of placing electronic devices pursuant to Title III electronic surveillance orders. In considering this issue, the Court reasoned that "absent covert entry . . . almost all electronic bugging would be impossible,"<sup>30</sup> a compellingly rational conclusion given that the entire purpose of wiretapping would be defeated if law enforcement officers were required to advise targets prior to implementing the electronic surveillance devices.

Several appellate courts have considered the issue of whether timely notice after surreptitiously executing a warrant is constitutionally required. For example, in the case of *United States v. Freitas*, the court determined that a warrant failing to explicitly provide for notice to the target at a reasonable time after the covert entry was constitutionally defective. According to the court,

surreptitious searches and seizures of intangibles strike at the very heart of the interests protected by the Fourth Amendment. The mere thought of strangers walking through and visually examining the center of our privacy interest, our home, arouses our passion for freedom as does nothing else. That passion, the true source of the Fourth Amendment, demands that surreptitious entries be closely circumscribed.<sup>31</sup>

Section 213 of the Patriot Act authorizes delayed notice to targets of sneak and peak warrants, but rather than incorporate a definite time period for notification, it permits “such notice within a reasonable period of [the warrant’s] execution, which period may thereafter be extended by the court for good cause shown.” Again, in this setting, the lack of definitional precision renders potential targets captive to the whims and creativities of law enforcement officials. The imagery of government officials surreptitiously entering private dwellings and rummaging through homeowners’ personal possessions is one that Americans have viewed in countless movies depicting the travails of everyday life under oppressive governmental regimes. Because of a strong constitutional foundation supporting personal privacy and limited governmental intervention, Americans hardly imagine that such outrageous conduct could occur in the United States. However, Section 213 of the Patriot Act threatens to convert remote film images into real cinema vérité on American shores.

When notice of covert entry into protected areas is delayed, Fourth Amendment protections are compromised in ways that can result in irreparable harm to the innocent and guilty alike. It is virtually impossible to challenge the scope of a search if one cannot meaningfully recreate the circumstances existing at the time of the search, particularly if no tangible items were seized. Moreover, notification long after the fact precludes targets from pointing out obvious deficiencies (e.g., wrong address) to law enforcement personnel at the scene. Perhaps most importantly, though, because sneak and peak warrants are not limited to investigations regarding terrorist activity but rather apply to *all* criminal investigations, every person within the jurisdictional reach of the statute now has reason to fear being victimized by these invasive techniques in an age of overzeal-

ous law enforcement purportedly aimed at fighting a war on terrorism.

### Threats to Due Process

The first several clauses of the Fourteenth Amendment of the U.S. Constitution state:

#### EQUAL JUSTICE in the balance

138

All persons born or naturalized in the United States and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

Because this language inexplicably categorizes protections for “citizens” as well as “any person,” the U.S. Supreme Court has on myriad occasions interpreted this language and defined its applicability to various classes of individuals. In the case of *Zadvydas v. Davis*, for example, the Court began by elucidating the general guidelines of Fourteenth Amendment protection, namely, that certain constitutional protections available to persons inside the United States are unavailable to noncitizens outside of its geographic borders.<sup>32</sup> The Court then explained, however, that once a noncitizen is within the United States his or her legal status changes along with safeguards provided under the Fourteenth Amendment. More specifically, the Due Process and Equal Protection Clauses apply to “all persons” within the United States and make no distinction based on citizenship or the legal status of one’s presence in the country. Similarly, in the case of *Yick Wo v. Hopkins*, the Court emphasized that

The Fourteenth Amendment to the Constitution is not confined to the protection of citizens. It says: “Nor shall any state deprive any person of life, liberty, or property without due process of law; nor deny to any person within its jurisdiction

the equal protection of the laws.” These provisions are universal in their application, to all persons within the territorial jurisdiction, without regard to any differences of race, of color, or of nationality; and the protection of the laws is a pledge of the protection of equal laws.<sup>33</sup>

Numerous provisions of the USA Patriot Act threaten the values inherent in these fundamental notions of due process and equal protection. For instance, Section 806, a new forfeiture provision, authorizes confiscation of all assets, foreign or domestic, of any individual, entity, or organization engaged in planning or perpetrating any act of domestic or international terrorism against the United States or their property. Furthermore, any property acquired, maintained, or derived from involvement with domestic or foreign terrorism activities is also subject to forfeiture to the U.S. government. To extend the act’s global reach, Section 319 provides for forfeiture of funds in interbank accounts. Essentially, any funds deposited in a foreign bank that has an interbank account with a U.S. bank are treated as if deposited in the United States for purposes of forfeiture rules. Presumably to reduce any unfairness and hardship that might result from this provision, the attorney general is authorized to suspend forfeiture proceedings when the “interests of justice” obviate the need for applying the “U.S. deposit presumption.” Traditionally, forfeiture is a tool utilized by the government to remove the economic underpinnings of criminal activity. The theory is, quite simply, that crime should not pay, and, therefore, to the extent that unlawful activities result in proceeds of any kind, those tainted profits are forfeitable to the government.<sup>34</sup> This remedy is exclusive of and in addition to any criminal sanctions that might be imposed. Over the years, numerous defendants stripped of their economic resources have challenged the constitutionality of criminal forfeiture. More specifically, defendants have alleged that, in some instances, the total dollar amount of the mandated forfeiture is excessive and, therefore, violative of the Eighth Amendment prohibition against excessive punishment. Moreover, because forfeiture is a separate remedy, often in addition to a period of incarceration, it is alleged to directly contravene the Fifth Amendment double jeopardy ban on multiple punishments for the same offense.

The U.S. Supreme Court has consistently rejected the double

jeopardy argument, noting that civil forfeiture sanctions assessed in conjunction with criminal penalties and based upon the same underlying events have been employed against criminals since the earliest days in America. According to the Court's reasoning, civil forfeiture proceedings do not violate double jeopardy standards because civil sanctions target the proceeds of the crime rather than the defendant, thus not exacting another personal punishment from the convicted person. However, with respect to the excessive punishment argument, the Court has determined that, when the case proceeds under a criminal forfeiture provision, the Eighth Amendment's Excessive Fines Clause limits the government's power to extract payments as punishment for an offense. Expressed differently, this means that the designated forfeiture must be proportional to the criminal conduct, a basic tenet of criminal law. The proportionality requirement is also applicable to civil forfeitures if it is determined that effectuation of the forfeiture imposes a punitive sanction in addition to the civil remedial component.

Section 806 of the USA Patriot Act is troublesome because it mandates forfeiture for conduct that is arguably at the outer limits of historically defined notions of criminality, if not completely outside the bounds altogether. For example, Section 806 authorizes forfeiture for any act of domestic or international terrorism. The newly enacted definition of *domestic terrorism* as set forth in Section 802 of the act describes domestic terrorism as activities that

- (A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;
- (B) appear to be intended—
  - (i) to intimidate or coerce a civilian population;
  - (ii) to influence the policy of a government by intimidation or coercion; or
  - (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and
- (C) occur primarily within the territorial jurisdiction of the United States.

On its face, this definition is far-reaching and consistent with other sections of the act lacking in precision. As such, application of Section 806 could result in the classification of legitimate political

dissent as terrorism, thereby subjecting participants to possible criminal convictions and forfeiture of assets for such conduct. Another basic tenet of criminal law requires that statutes be drafted in a manner that gives citizens fair notice of prohibited conduct, so that they may conform their conduct to the dictates of the law. As Nancy Chang, senior litigation attorney at the Center for Constitutional Rights, observes of Section 802:

Because this crime is couched in such vague and expansive terms, it may well be read by federal law enforcement agencies as licensing the investigation and surveillance of political activists and organizations based on their opposition to government policies. It also may be read by prosecutors as licensing the criminalization of legitimate political dissent. Vigorous protest activities, by their very nature, could be construed as acts that “appear to be intended . . . to influence the policy of a government by intimidation or coercion.” Further, clashes between demonstrators and police officers and acts of civil disobedience—even those that do not result in injuries and are entirely non-violent—could be construed as “dangerous to human life” and in “violation of the criminal laws.” Environmental activists, anti-globalization activists, and anti-abortion activists who use direct action to further their political agendas are particularly vulnerable to prosecution as “domestic terrorists.”<sup>35</sup>

Also of particular note with respect to Section 806 is its failure to include a conviction requirement prior to imposition of its draconian forfeiture standards. Thus, an indictment or even perhaps an arrest for “domestic terrorism” can arguably trigger the application of the forfeiture statute. As a final example of the stringent nature of Section 806, it entirely omits the typical requirement that forfeited assets be tied to criminal or terrorist activity. Instead, it is sufficient if the property was owned or possessed by the alleged terrorist at the time of the suspected illegal conduct. The very fact that these proposed forfeitures are, on their face, inexact and excessively punitive negates any conclusion that they are designed to serve an underlying remedial purpose and creates a constitutional conundrum that may, before long, require judicial intervention. In the

end, to quote the fateful words of Senator Patrick Leahy, "Congress may have to revisit these issues."

### Indefinite Detention and Deportation

**EQUAL JUSTICE**  
in the balance

142

Prior to the enactment of the USA Patriot Act, immigration legislation provided that noncitizens could be excluded from the United States for a number of reasons, including having prior criminal activity and exhibiting behavior that may pose a threat to the health or safety of others. Section 411 of the Patriot Act expands the grounds for exclusion to include categories such as being a representative of a political, social, or other similar group whose public endorsements of terrorist activities undermine U.S. efforts to reduce or eliminate terrorism; being a spouse or child of an inadmissible alien associated with terrorist activity within the past five years; and being an alien who uses a position of prominence within *any* country to endorse or espouse terrorist activity. Those who associate with terrorist organizations and intend "while in the United States to engage solely, principally or incidentally in activities that could endanger the welfare, safety or security of the United States" are also inadmissible. The determination of whether one has associated with a terrorist is left to the discretion of "the Secretary of State, after consultation with the Attorney General, or the Attorney General, after consultation with the Secretary of State." Section 411 of the act also defines "engage in terrorist activity" to comprise such a broad category of conduct that it is difficult, if not impossible, to meaningfully distinguish legitimate and constitutionally protected political dissent from unlawful terrorist activities. For example, one such clause, which is hopelessly mired in ambiguity, defines "engaging in terrorist activity" to include committing

an act that the actor knows, or reasonably should know, affords material support, including a safe house, transportation, communications, funds, transfer of funds or other material financial benefit, false documentation or identification, weapons (including chemical, biological, or radiological weapons), explosives, or training . . . to a terrorist organization . . . unless the actor can demonstrate that he did not know, and

should not reasonably have known, that the act would further the organization's terrorist activity.

The use of phrases such as "reasonably should know" and "material support" grants wide latitude to the executive branch to declare open season upon disfavored immigrants for conduct as innocent as lending money or a means of transportation to a friend who is later determined to be affiliated with a terrorist organization. Moreover, even if an immigrant has knowledge of a friend's association with a terrorist organization, the statute provides no reasonable yardstick for measuring when the critical "material support" threshold has been crossed. Thus, this clause looms like a dark cloud over the legitimate associations and private friendships of legal immigrants in America, potentially resulting in unnecessary self-monitoring and limitations on lawful conduct lest it be taken as "material support."

The USA  
Patriot Act  
143

But the coup de grâce to fair notice and due process, and a shining example of executive hubris masquerading as legislation, is contained in the final paragraph of this clause:

This clause shall not apply to any material support the alien afforded to an organization or individual that has committed terrorist activity, if the Secretary of State, after consultation with the Attorney General, or the Attorney General, after consultation with the Secretary of State, concludes in his *sole unreviewable discretion*, that this clause should not apply. [emphasis added]

Granting the executive branch ultimate authority to determine who falls within and without the boundaries of engaging in terrorist activity is eerily reminiscent of a duo of U.S. legislative enactments passed during the latter part of the eighteenth century as the fledgling country stood on the precipice of war with France. The Alien Act of 1798 gave the president broad authority to deport those aliens deemed dangerous to the peace and safety of the United States or those suspected of treasonable or secret machinations against the government. Its partner statute, the Sedition Act of 1798, made it unlawful for any person to write, print, utter, or publish any false, scandalous, and malicious writings about the government

with the intent to defame or bring the government into contempt or disrepute or to excite the hatred of the people against America. Ostensibly designed to protect American shores from enemy infiltration during a time of heightened national security concern, these acts were eventually used to suppress the largely Democratic-Republican immigrant vote and to quell domestic political dissent, particularly viewpoints that attacked the Federalist Party agenda. Fifteen people were indicted under the Sedition Act, resulting in ten convictions; all of them were Democratic-Republicans, who were assessed heavy fines and imprisoned. While no aliens were deported or taken into custody under these statutes, immigrants fled American shores in large numbers, fearing eventual arrest, detainment, and deportation. Subsequent public backlash against the Federalist Party for its role in creating such repressive legislation spelled the end of that party and heralded the emergence of the Democratic-Republicans, the nation's first opposition party.

Since 9/11, the executive branch has adopted a decidedly ahistorical approach to addressing the undeclared war on terrorism, ignoring, in practically every instance, lessons from the past that dictate caution over excess in times of crisis. Although unsuccessful in his effort to defeat the Alien and Sedition Acts over two centuries ago, Senator Edward Livingston nevertheless exposed the insidious contradiction that necessarily obtains when a nation purportedly committed to the highest principles of democracy takes a repressive stance toward its own people under the guise of protecting national security:

Do not let us be told that we are to excite a fervor against a foreign aggression to establish a tyranny at home; that like the arch traitor we cry "Hail Columbia" at the moment we are betraying her to destruction; that we sing "Happy Land," when we are plunging it in ruin and disgrace; and that we are absurd enough to call ourselves free and enlightened while we advocate principles that would have disgraced the age of Gothic barbarity.<sup>36</sup>

Section 412 authorizes the attorney general to detain alien terrorist suspects for up to seven days upon certification that reasonable grounds exist to believe that they are engaged in conduct that

threatens the national security of the United States or are inadmissible or deportable for other terrorist-related reasons. Within this seven-day window, the attorney general must formally commence proceedings against the detainee designed to effectuate removal from the country or initiation of a criminal prosecution. Failure to comply with the Patriot Act's version of the "speedy trial rule" will result in the detainee's release from custody. However, an alien who has not been removed from the country, and whose removal is unlikely in the foreseeable future, "may be detained for additional periods of up to six months . . . if the release of the alien will threaten the national security of the United States or the safety of the community or any person." If the detainee is held for longer periods of time, the attorney general is required to review the certification every six months, and "if the Attorney General determines, *in the Attorney General's discretion*, that the certification should be revoked, the alien may be released on such conditions as the Attorney General deems appropriate, unless such release is otherwise prohibited by law" (emphasis added). The alien may also request a reconsideration of the certification every six months and may submit documents or other evidence in support of the request. The attorney general's determinations are subject to review only under federal writs of habeas corpus, with a limited right of appeal to the United States Court of Appeals for the District of Columbia. As a paean to congressional oversight, the attorney general must file a biannual report to the Committee on the Judiciary in both the Senate and House of Representatives.

This section of the Patriot Act is in apparent conflict with the military order issued by President Bush on November 13, 2001, which, by its terms, applies to the same category of noncitizens as contemplated by Section 412. Such an obvious conflict is highly indicative of the haste with which Congress enacted this legislation, failing at the most basic level to determine whether other standards were being contemplated to address the conduct described in Section 412. The military order, entitled "Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terrorism," states in pertinent part that

the term "individual subject to this order" shall mean any individual who is not a United States citizen with respect to

whom [the President determines] from time to time in writing that:

- (1) there is reason to believe that such individual, at the relevant times,
  - (i) is or was a member of the organization known as al Qaeda;
  - (ii) has engaged in, aided or abetted, or conspired to commit, acts of international terrorism, or acts in preparation therefor, that have caused, threaten to cause, or have as their aim to cause, injury to or adverse effects on the United States, its citizens, national security, foreign policy, or economy; or
  - (iii) has knowingly harbored one or more individuals described in subparagraphs (i) or (ii) of subsection 2(a)(1) of this order; and
- (2) it is in the interest of the United States that such individual be subject to this order.

According to the order, individuals subject to its provisions may be detained at an appropriate location designated by the secretary of defense outside or within the United States; treated humanely; afforded adequate food, shelter, clothing, and medical treatment; and allowed to practice their religion. When tried for their alleged crimes, military tribunals

shall have exclusive jurisdiction with respect to offenses by the individual; and . . . the individual shall not be privileged to seek any remedy or maintain any proceeding, directly or indirectly, or to have any such remedy or proceeding sought on the individual's behalf, in . . . any court of the United States, or any State thereof, any court of any foreign nation, or any international tribunal.

There is an apparent definitional overlap between Section 412 and the military order concerning the categories of individuals who might fall within the jurisdiction of each. Specifically, "aliens who endanger national security" under Section 412 may also be "those engaged in, assisting or conspiring to commit acts of international

**TABLE 2. Key Differences between Section 412 of the USA Patriot Act and the President’s Military Order**

	Individuals Covered	Length of Detention	Decision Making	Forum	Appellate Review
USA Patriot Act, Section 412	Aliens who endanger national security or are inadmissible or deportable for other terrorist-related reasons	Not longer than seven days without proceedings; if can’t be removed from country and will be a threat to national security, then may be detained for up to six months	Attorney general certifies based on “reasonable grounds”; may delegate power to deputy attorney general	U.S. federal courts	Habeas corpus proceeding, which may only be appealed to U.S. Court of Appeals for District of Columbia
Military Order	Current or former al-Qaeda members; those engaged in, assisting with, or conspiring to commit acts of international terrorism against the U.S.; those knowingly harboring terrorists	Indefinite	President determines based on “reason to believe”	Military commissions	Three-member review panel appointed by secretary of defense; president makes final decision

terrorism” under the military order. Uncertainty as to which mandate is applicable in any given situation gives the government wide latitude to impose dramatically different punishments on similarly situated individuals. That is, under Section 412, a semblance of due process prevails. The government must comply with time limitations or risk release, a detainee is entitled to access the federal court system, and the government is required to justify its detainment on a biannual basis. In sharp contrast, detainment under the military order as currently implemented condemns a detainee indefinitely to Guantanamo Bay, Cuba, a “permanent penal colony for the human detritus of the campaign against terrorism.”<sup>37</sup>

Although noncitizens have been detained under both standards, it is nevertheless unclear whether these interrelated mandates will operate exclusively or in tandem. One could well imagine that, in our current environment, where lengthy detainments of noncitizens on sparse evidence are apparently symbolic of fighting the war on terrorism, it would not be beyond the pale for the government to strategically use both provisions to justify political objectives.

### **Challenges Ahead**

We were warned thirty years ago about the vicissitudes and inherent dangers of unfettered governmental authority wielded indiscriminately against innocent citizens in the name of national security. After the September 11 tragedy, the DOJ, in a blatant attempt to seize power in a moment of national crisis, struck swiftly and decisively, giving Congress a wish list of proposed legislation calling for unprecedented governmental intervention into the lives of citizens and noncitizens alike. Congress, still deciphering the impact of the 9/11 attacks and feeling pressure from constituents to “do something,” blindly caved in to the wishes of the executive branch, ceding nearly all of its oversight authority, lest its members appear unpatriotic at a time when patriotism is seemingly defined by one’s ability to submit without question to governmental authority for the sake of national cohesiveness. The USA Patriot Act was the legislative result, and, while its impact is still largely unknown, initial assessments do not bode well.<sup>38</sup> There are some, however, who believe that Patriot Act naysayers are alarmists and are making

much ado about nothing. Yet, in 2002, the previously silent FISA court spoke publicly for the first time, revealing that it is not so dismissive of these concerns.

Consistent with his interpretation of the broad grant of authority in the Patriot Act, in March 2002 the attorney general filed a motion with the FISA court requesting that the court now grant orders for electronic surveillance and physical searches if the investigation is “primarily for a law enforcement purpose, so long as a significant foreign intelligence purpose remains.”<sup>39</sup> In response, the court first noted that its duty in reviewing FISA surveillance requests is to “ensure that the intrusiveness of foreign intelligence surveillances and searches on the privacy of U.S. persons is ‘consistent’ with the need of the United States to collect foreign intelligence information from foreign powers and their agents.”<sup>40</sup> Explaining how this function is accomplished, the court observed that, “[i]n order to preserve both the appearance and the fact that FISA surveillance and searches were not being used *sub rosa* for criminal investigations, the Court routinely approve[s] the use of information screening ‘walls,’”<sup>41</sup> which restrict the flow of information between foreign intelligence agents and criminal investigators.<sup>42</sup>

Against this backdrop, the court examined the attorney general’s motion for expanded exchange of information, concluding that, according to the attorney general’s interpretation, “criminal prosecutors are to have a significant role *directing* FISA surveillances and searches from start to finish in counterintelligence cases having overlapping intelligence and criminal investigations or interests, guiding them to criminal prosecution.”<sup>43</sup> The court opined that this may be “because the government is unable to meet the substantive requirements of these law enforcement tools, or because their administrative burdens are too onerous,” but stressed that the court was not persuaded by such justifications.<sup>44</sup> In denying the government’s request for unrestricted sharing of information, the court ordered that

law enforcement officials shall not make recommendations to intelligence officials concerning the initiation, operation, continuation or expansion of FISA searches or surveillance. Additionally, the FBI and the Criminal Division shall ensure that law enforcement officials do not direct or control the use of the

FISA procedures to enhance criminal prosecution, and that advice intended to preserve the option of a criminal prosecution does not inadvertently result in the Criminal Division's directing or controlling the investigation using FISA searches and surveillances toward law enforcement objectives.<sup>45</sup>

After the ruling, Senator Patrick Leahy lauded the decision, observing that this "ray of sunshine from the judicial branch is a remarkable step forward for constructive oversight . . . and [provides] a window on the process that will help us better understand how the laws are being implemented and how well they are working." As to its long-term impact, Leahy predicted that the FISA court ruling might "save the Justice Department from overstepping constitutional bounds in ways that could have dire consequences in our most serious national security cases."<sup>46</sup>

Despite Senator Leahy's guarded optimism, at this writing, the Center for Public Integrity, a nonpartisan organization dedicated to "public service journalism," has disclosed to the media a document that outlines a new DOJ wish list, apparently designed to expand upon the powers already granted in the Patriot Act. Ominously labeled "Patriot II," the document proposes, among other things, the expansion of power to wiretap American citizens, easier governmental access to credit reports and financial information, and the voluntary loss of American citizenship for anyone found to have materially supported a hostile terrorist organization. Although none of these provisions has been formally proposed to Congress, they, like the abandoned TIPS program, are indicative of the current executive branch ethos that cavalierly abandons civil liberties in the name of national security. When asked about the leaked Patriot II document, Attorney General Ashcroft responded, "Percolating ideas into the system is very important."<sup>47</sup>

As the Patriot Act nears its two-year anniversary, there is little cause for celebration as individuals and organizations spanning the political spectrum are mounting numerous challenges to the act's expansive provisions across the country. This escalating backlash includes nearly 150 state and local governments that have each passed legislation condemning the act and, in some instances, have refused to enforce its provisions. In July 2003 the American Civil Liberties Union (ACLU) filed a lawsuit in the U.S. district court in

Michigan alleging that Section 215 of the Patriot Act, which authorizes searches of business, library, and bookstore records, is unconstitutional and being used primarily to target individuals based upon ethnicity, religion, and political associations.

There is also growing resistance in Congress, as the House recently voted 309 to 118 to discontinue funding for governmental activities that facilitate the sneak and peek warrant provision of the act. In addition, a more sweeping revision of the act is currently being proposed as Congress attempts to rein in some of its more constitutionally questionable provisions. Senator Lisa Murkowski introduced legislation in August 2003 designed to provide greater definition for the expanded powers in the act and to ensure that the law is working as intended. Among other things, Senator Murkowski's bill seeks to

- Ensure that only an individual who has violated one of the federal crimes of terrorism while operating within the jurisdiction of the United States could be designated as a domestic terrorist
- Permit intelligence agencies to seek warrants for a broad range of evidence, but require a showing of "reasonable cause" that the individual to whom the records pertain is a foreign power or an agent of a foreign power
- Raise the standard for the government to look at medical records, library records or records involving the purchase or rental of books, videos and music by requiring the government to show "probable cause" to gain such search powers
- Ensure that libraries will not be required to turn over Internet usage information about their patrons, unless the government meets the standards required by the Foreign Intelligence Surveillance Act
- Require a court order approving an electronic surveillance to specify either the identity of the target or the location of the facility where the surveillance will occur
- Add judicial review for "pen registers" and "trap and trace" device requests by requiring that the government show specific facts that indicate that a crime has been, is, or will be committed

- Define the types of Internet usage and email information that can be obtained
- Require greater public reporting on activities conducted under the Foreign Intelligence Surveillance Act (FISA)
- Apply discovery procedures already in place under the Classified Information Procedures Act (CIPA) to other court proceedings that will use evidence collected under FISA
- Restore the former requirement that the “primary purpose” for electronic surveillance and physical searches under the Foreign Intelligence Surveillance Act is to obtain foreign intelligence
- Provide for greater judicial review of government requests for educational records by requiring the government to set forth specific facts indicating the education records are relevant to an investigation.<sup>48</sup>

Despite the intensifying challenges, Attorney General Ashcroft and FBI director Mueller continue to vigorously support the act as a critical tool in the war against terrorism, albeit with persistent reluctance to submit their activities to congressional scrutiny. In May 2003, under pressure from Congress, the DOJ revealed that, under the Patriot Act provisions, it had detained fewer than fifty people as material witnesses without charging them and had received only forty-seven delayed notification search warrants. However, the report also indicated that the act’s provisions were being used for nonterrorism-related cases including securing the forfeiture of assets from a lawyer who absconded with client funds. The report, however, did not provide specific information on the number of libraries that had been approached for patron records.

A later report released in July 2003 by the DOJ’s inspector general’s office revealed that 1,073 new complaints of civil rights and civil liberties violations have arisen under the Patriot Act, 34 of which were deemed “credible.” According to the report, these abuses range from abusive treatment by prison officials to unlawful searches of prison cells and private residences.<sup>49</sup> In an effort to quell resistance, the DOJ is currently planning what amounts to a USA Patriot Act public relations tour purportedly to set the record straight as to how the act’s provisions are being used to effectively

wage the war against terrorism. However, this effort may be too little too late. As widespread resistance to the Patriot Act's more egregious provisions increases, it is perhaps inevitable that Americans through their democratic institutions will restore the balance between national security and civil liberties and return the reason, sense of fair play, freedom, and respect for others that served as the impetus for founding a great nation more than two centuries ago.

**The USA  
Patriot Act**

**153**