American Bar Association

National Security Law Report

Volume 26, Number 4 STANDING COMMITTEE ON LAW AND NATIONAL SECURITY November 2004

A Practical History of the USA PATRIOT Act

Michael J. Woods

The USA PATRIOT Act has sparked intense public debate, with proponents claiming that the Act is a necessarily hard-minded response to a national crisis, while opponents see unwarranted, even opportunistic, expansion of state power. Perhaps no provision of the Act has generated more controversy than §215, which authorizes the FBI to seek a court order compelling the production of "any tangible things" relevant to certain counterintelligence and counterterrorism investigations. Like many other provisions of the USA PATRIOT Act, §215 will expire on December 31, 2005, unless reauthorized by Congress. The controversy, therefore, is likely to intensify over the coming year.

The rhetoric swirling about this provision has been extreme, despite the paucity of evidence that it has ever actually been used—which suggests that the section is neither the deadly threat to civil liberties nor the vital operational necessity that its detractors and defenders, respectively, contend. Section 215, removed from its context in national security law, might be regarded as ominous, but placed in the larger context of operational counterintelligence authorities for access to transactional information, it emerges as an understandable, though arguably incomplete, evolutionary step.

A Short History of Statutory Authorities for Counterintelligence Investigations

A full understanding of §215 begins with the role of counterintelligence within the larger landscape of national security law. National security law includes a range of authorities granted to the executive branch for the defense of the nation. These legal authorities, subject to congressional regulation and oversight, are the basis for military operations, the collection of foreign intelligence, and covert activities. "Counterintelligence" describes a subset of these activities, those conducted to protect against espionage and

Continued on page 2

INSIDE THIS ISSUE

FRIEDMAN APPOINTED CHAIR

Advisory Committee Members Selected

The Advisory Committee of the ABA Standing Committee on Law and National Security serves alongside the Committee to provide research and advice on national security law issues. ABA President Robert Grey has appointed **Richard Friedman** as Chair. Friedman is President and Chair of the National Strategy Forum in Chicago.

Other appointments to the Advisory Committee include: **Zoe Baird,** President of the Markle Foundation; **Richard Blau** in private practice in Florida; **John Cooke,** Director, Judicial Education Division, Federal Judicial Center; **Mary DeRosa,** Senior Fellow, Technology and Public Policy Program, Center for Strategic and International Studies; **Viet Dinh,** Professor of Law and Deputy Director, Asian Law & Policy Studies Program at Georgetown University Law Center; **James Durant,** Major, United States Air Force; **Stephen Dycus,** Professor of Law, Vermont Law School and co-author of the National Security Law textbook; **Gordon Lederman,** Professional Staff, Senate Committee on Government Affairs; **Josh Levy,** Counsel, Office of Senator Charles Schumer; **James McDaniel,** private practice in St. Louis, Missouri; **Elizabeth Rindskopf Parker,** Dean, University of the Pacific McGeorge School of Law; **Vincent Polley,** private practice in Houston, Texas; **Jonathan Scharfen,** Chief Counsel, House International Relations Committee; **Walter Gary Sharp,** Director, Legal Research for International Comparative and Foreign Law at the Library of Congress; **Suzanne Spaulding,** former Staff Director, House Permanent Select Committee on Intelligence and former Director of the National Commission on Terrorism; **Paul Schott Stevens,** President, Investment Company Institute; **Michael Smith,** Booz-Allen Hamilton; **Ruth Wedgwood,** Professor, Johns Hopkins University School of Advanced International Studies; **Charles White,** Vice President, Administration, Business Leasing Associates; **John Yoo,** Professor of Law, University of California at Berkeley; and **Lee Zeichner,** private practice, Falls Church, VA.

We wish to thank those departing Advisory Committee members who have served the Committee so well: **Judge James Baker, Professor Lori Fisler Damrosch, Judith Miller, Steve Preston, Richard Thornburgh, Theresa Van**

Continued on page 9

PATRIOT Act. . .

Continued from page 1

international terrorism committed by foreign powers, organizations, or individuals. Counterintelligence within the United States is primarily the responsibility of the FBI, which conducts counterintelligence operations under guidelines issued by the Attorney General. Counterintelligence operations occur outside the structure of the criminal law, although they may lead to criminal prosecutions for espionage or terrorism-related crimes.

Historically, counterintelligence operations were subject to very little oversight. However, the revelation of abuses committed by the FBI, CIA, and DOD during the 1960s and 1970s prompted Congress to bring counterintelligence activities under a higher degree of regulation. The use of electronic surveillance in counterintelligence became subject to the Foreign Intelligence Surveillance Act of 1978 (FISA), which set boundaries on use of the technique and introduced judicial supervision. The same era saw the beginning of substantial executive branch regulation of U.S. counterintelligence and foreign intelligence activities.

One legacy of this period is an enduring concern that the tools available to counterintelligence should not be used to subvert the constitutional protections of the criminal law. This concern, which had its roots in pre-FISA case law, led to the creation of a "wall," built of legal and policy requirements and reinforced by culture, that separated counterintelligence officers from criminal investigators. But the wall, prior to its partial dismantlement through the operation of the USA PATRIOT Act and a subsequent court decision, had the unintended consequence of depriving counterintelligence operators of some of the basic tools of criminal investigation.

FBI counterintelligence agents were authorized by FISA to conduct electronic surveillance and physical searches. However, such methods are generally used only in the end stages of an investigation, after the probable cause required for FISA surveillance is established through the use of less intrusive techniques. Among those techniques are "national security letters"—a process by which counterintelligence agents obtain transactional information about investigative subjects. "Transactional" information broadly describes information that documents financial or communications transactions without necessarily revealing the substance of those transactions. Telephone billing records that list the numbers dialed by a particular subscriber, records from an Internet service provider showing when a user logged onto an account or to whom the user sent email, records of bank accounts or transfers of money between financial institutions, and credit records are all examples of transactional information.

The legal status of transactional information has evolved dramatically since the mid-1970s, following public awareness that nearly all transactional information resides beyond the protections of the Fourth Amendment. In *United States v. Miller* (1976), the Supreme Court held that the government can use a grand jury subpoena to obtain a defendant's financial records from a bank without violating the Fourth

Continued on page 8

The *National Security Law Report* is pleased to present two articles that will appear in the forthcoming inaugural issue of the *Journal of National Security Law & Policy*. Robert Chesney's article on the rhetoric and reality of the War on Terrorism will appear as a book review of *Terrorism, Freedom, and Security* by Philip B. Heymann. Both his review and the article by Michael J. Woods on the USA PATRIOT Act will appear in the *JNSL&P* with greater development of the issues and with complete legal citations.

The *Journal of National Security Law & Policy* is a new peer-reviewed law journal inspired by Dean Elizabeth Rindskopf Parker of The University of the Pacific, McGeorge School of Law. It will be edited by Professor Stephen Dycus of Vermont Law School and Professor John Cary Sims of Pacific/McGeorge. The *JNSL&P* will involve faculty at a number of law schools, as well as government and private attorneys specializing in national security issues.

The *JNSL&P* will be published twice a year at a subscription rate of $30 per year. The first issue will be published in 2004, and anyone subscribing as an inaugural member will receive that issue, and as a bonus, the two issues for 2005. Send subscription requests to Professor John Cary Sims, University of the Pacific, McGeorge School of Law, 3200 Fifth Avenue, Sacramento, CA 95817. The telephone number is (916) 739-7017. Email should go to jsims@pacific.edu.

THE ABA NATIONAL SECURITY LAW REPORT
<http://www.abanet.org/natsecurity/>

The *National Security Law Report* (*N.S.L.R.*) contains articles concerning the law relating to the security of our Nation and associated topics. The *N.S.L.R.* is sponsored by the ABA Standing Committee on Law and National Security. The views expressed in this publication are not necessarily those of the Standing Committee, the ABA, or any governmental agency or private enterprise.

To receive the *N.S.L.R.*, contact Holly Stewart McMahon at 740 15th St., NW, Washington, DC 20005-1009; (202) 662-1035; FAX (202) 662-1032; or hmcmahon@staff.abanet.org.

Rhetoric, Practice, and Historical Perspective in the War on Terrorism

Robert M. Chesney

I. The New Bipartisan Consensus

On the afternoon of September 11th, shortly after Air Force One touched down at Offutt Air Force Base, President Bush began a teleconference with senior national security officials by proclaiming "We're at war." The war, the president elaborated, would be "global in nature." During a meeting of the National Security Council the next day, the principals labored to flesh out the parameters of the conflict. In particular, they debated a proposal to frame America's objective not merely as the destruction of al Qaeda but as the "'elimination of terrorism as a threat to our way of life,' an aim that would include pursuing other international terrorist organizations in the Middle East."

The fruits of these discussions became clear when President Bush addressed Congress on the night of September 20, 2001. He identified the 9/11 attacks as acts of belligerency, albeit horribly unlawful ones, and declared al Qaeda's responsibility for them. But he also emphasized that al Qaeda was "linked to many other organizations in different countries," forming a "radical network of terrorists" along with supporting entities such as the Taliban. Thus, the President concluded, although the "war on terrorism begins with al Qaeda . . . [i]t will not end until every terrorist group of global reach has been found, stopped and defeated." The United States would, he added, use "every means of diplomacy, every tool of intelligence, every instrument of law enforcement, every financial influence, and every necessary weapon of war."

According to one observer, "whether it is appropriate to declare a war on terrorism is a question that's been debated almost continually since September 11th, 2001." Notwithstanding such debate, however, there is reason to believe that a bipartisan consensus has emerged regarding the propriety of the offensive use of military force against terrorists in at least some circumstances. Thus we find the major presidential candidates vigorously disputing the manner in which the Bush Administration has used military force since 9/11 in the name of fighting terrorism, but not the general principle that military force should play a very significant role in counterterrorism policy (in this essay, I use the phrase "counterterrorism policy" to refer broadly to the full array of terrorism-related policies).

This is a remarkable development, all the more so when viewed in historical perspective. The phrase "war on terrorism" has become so ubiquitous since 9/11, so intimately associated with the policies of the Bush Administration, that most of us seem to have forgotten that American presidents of both parties have been declaring "war on terrorism" with great frequency and earnestness for some twenty years now. The actual practice of counterterrorism policy did not live up to this rhetoric prior to 9/11, however. Notwithstanding the views of some government officials urging greater reliance on military force as an instrument of counterterrorism policy during that period, military force in fact was employed only in rare, retaliatory circumstances.

II. The Gap Between Rhetoric and Practice Prior to 9/11

Perhaps the earliest manifestation of the tendency of politicians to invoke the imagery of war to represent and reinforce their commitment to counterterrorism arose in the early 1980s in the wake of the Hezbollah and al Dawa bombings of U.S. embassies and military installations in Beirut and Kuwait. These events generated sharp debate within the Reagan Administration regarding the use of military force against terrorist organizations and their state sponsors. Two cabinet members – Secretary of State George Shultz and Secretary of Defense Casper Weinberger – presented the opposing perspectives. Secretary Shultz took the view that "terrorism was a form of warfare for which we were ill prepared," and advocated the use of force for purposes of "active prevention, preemption, and retaliation." As an observer reported, Shultz on one occasion "was actually shouting his insistence that we 'wake up' to terrorism as 'an international form of warfare . . . directed largely against us and our way of life.'" Shultz, in short, was calling for the government to "use [its] power to fight the war against terrorism" in literal terms.

Secretary Weinberger acted as a brake on Shultz's enthusiasm. Sounding themes with considerable resonance at a time when memories of Vietnam remained fresh, Weinberger frequently warned against the precipitate use of military force. In a summary of his views offered in connection with the U.S. airstrike against Libya, for example, Weinberger noted that it "is tempting for many to exploit our renewed military strength," but that military force "should be used only when we have, and can achieve, a proper objective" and "should never be used except as a last resort, and when all else has failed. Military forces should certainly not be used on any occasion unless a matter of major national importance is involved." According to then-National Security Advisor Robert McFarlane, Weinberger felt these conditions simply were not met with respect to the complex diplomatic, political, and military circumstances America confronted with respect to terrorism in the Middle East in the early 1980s.

Continued on page 4

War on Terrorism

Continued from page 3

This debate was not merely internal to the administration. Shultz's vigorous public statements followed a message to Congress from President Reagan describing a "war against terrorism," and both support and criticism from the media followed. *The Wall Street Journal*, for example, editorialized in favor of the Shultz view that this "war" should be fought with offensive force, writing that Shultz "was right to say again last week that the war against terrorism will begin only if the West has the will to fight this fire with fire." The *Washington Post*, in contrast, vigorously asserted the contrary view. Richard Cohen of the *Post* argued that "even retaliation . . . would not substantially change matters" and that the "war on terrorism" rhetoric masked the reality that military force "either cannot be applied or dares not be applied." Meg Greenfield, also of the *Post*, echoed Cohen, arguing that the phrase "'war' with terrorism" is an "especially unfortunate formulation," and that war is "exactly what we are not in." Greenfield wrote that the effect of using such language in connection with terrorism "is to elevate these grubby criminal acts to a status they don't deserve; it is to cast at least indirectly, all Americans as enemy civilians or belligerents and thus fair game; and it is to misdescribe the nature of the assault itself."

Such criticisms did not dissuade President Reagan from continuing to deploy the language of a "war on terrorism" for rhetorical purposes in the following years. During the same period, moreover, a number of books began to use the language of the "war on terrorism" in connection with analyses of U.S. counterterrorism policy. But the reality of that policy did not quite live up to the martial rhetoric. As a practical matter, military force was used only sparingly in the counterterrorist context in those years.

This pattern continued into the Clinton administration, with the rhetoric of war surfacing frequently in connection with terrorism while in practice counterterrorism remained firmly within the domain of the diplomats, the intelligence agencies, and the prosecutors. In a May 1995 radio address not long after the Oklahoma City bombing, for example, President Clinton urged Congress to pass pending terrorism legislation, warning that "[w]e mustn't let our country fight the war against terrorism ill-armed or ill-prepared." Likewise, in the aftermath of the bombing in Dharan, Saudi Arabia, we find State Department spokesman Nicholas Burns reminding reporters that "we believe we're in a war against terrorism, as the president said."

The continued rhetorical invocation of a war paradigm in the 1990s eventually raised questions. Did we mean war in the literal sense of an increased reliance on military operations in the terrorism context, or was this just an organizing motif meant to lend oomph to the traditional blend of diplomatic, legal, and intelligence efforts? At least in the mid-1990s, the answer seemed to be that it was merely a rhetorical device akin to the "war on drugs," in keeping with past policy trends. According to the Democratic Party Platform upon which President Clinton successfully sought reelection in 1996, for example, the "war on terrorism" (also referred to in the platform as the "war on global terrorism") had "three front[s]." None involved military force. Instead, the "war" was to be carried out "abroad, through greater cooperation with our allies; at home, by giving law enforcement the most powerful tools available to fight terrorism; and in our airports and on airplanes, through tough air travel security measures . . . ."

After the al Qaeda truck bombings of our embassies in Nairobi and Dar es Salaam in 1998, however, it appeared for a time that the "war on terrorism" might begin to incorporate military force on a more sustained basis. Initially, the Clinton administration was pointedly noncommittal. Thus we find Colonel P.J. Crowley, the National Security Council's Senior Director for Public Affairs, refusing to let reporters pin him down on the topic:

> Q: Are we in a state of war – we have a war on drugs. Are we in a state of war against terrorism, or does that require a declaration in order for us to fight?
>
> A: I think we see terrorism as the emergent threat of the '90s. It will be the major threat that America faces globally into the next century.
>
> Q: Are we in a state of war against it so that we can fight these people if we can't apprehend them?
>
> A: I think we recognize the dangers and we're taking appropriate steps to address them.

But the uncertainty seemed to lift later in the month after the United States launched cruise missiles against targets in Afghanistan and the Sudan in retaliation for the embassy bombings. A "senior Pentagon official" at that time warned that "this is not a one-shot deal here . . . we are engaged in a different – a real war against terrorism."

Unfortunately, it was in fact a "one-shot deal." We know now that efforts were made in the 1998-99 period by many officials within the Clinton Administration and the military – most notably, Richard Clarke of the National Security Council, General Peter Schoomaker of Special Operations Command, and Thomas Kuster of the Office of the Assistant Secretary for Special Operations and Low-Intensity Conflict – who sought to go beyond the initial August missile strikes and to become more aggressive with the use of military force to disrupt al Qaeda and to kill its leaders and operatives. But despite their efforts, the missile strikes of August 1998 would be the last overt use of military force against terrorists until after 9/11.

A number of factors combined to block further military action. Some had considerable force, even in retrospect, while others seem to reflect what proved to be a mistaken assessment of the magnitude of the threat posed by al Qaeda: the lack of "actionable intelligence" regarding bin Ladin's location; the certainty of escalating international hostility against the U.S. (and some degree of domestic hostility as

well) at a time when we already were involved in the use of force in Iraq and Kosovo; uncertainty about the overflight and basing rights necessary for such critical activities as search-and-rescue operations; and, most disconcertingly, domestic political constraints arising both from "wag the dog" allegations linked to the Lewinsky scandal and from still-disputed claims about the accuracy of the intelligence upon which the initial strike was based.

Neither the subsequent bombing of the *USS Cole* in 2000 nor the discovery of al Qaeda plots to attack American targets at the millennium in Los Angeles and Amman, Jordan, resulted in a military response in the final days of the Clinton Administration or the early days of the Bush Administration. In both instances difficult questions about attribution of responsibility for the attacks (and meta-questions about the standard of proof to be applied in deciding attribution) added to the factors cited above in preventing military responses to them. The use of military force in August 1998 thus represented an exception to the status quo rather than the emergence of a true "war" on terrorism, much like the isolated use of airstrikes against Libya in 1986. The war rhetoric remained in circulation in those final years, but would not be borne out in literal terms until after 9/11.

In summary, the concept of a "war on terrorism" has been a rhetorical staple in continuous usage by government officials and commentators alike since at least the early 1980s. Prior to 9/11, however, the phrase was little more than a marshaling device. Notwithstanding the efforts of individual proponents of more aggressive action, military force in this period played only a minor and episodic role in counterterrorism policy compared to the instruments of diplomacy, law enforcement, and intelligence gathering. The Bush Administration's robust embrace of military mechanisms after 9/11 thus involved continuity of rhetoric, but a sharp break with the past in terms of actual practice.

III. The Limits of Consensus

The post-9/11 bipartisan consensus in support of the general principle that military force can and should be used against terrorists will serve to entrench this policy shift. This is an immensely important development, marking the demise of a significant hurdle to a more effective counterterrorism policy. But it certainly does not signal the end of serious debate regarding the details of the military's role in the war on terrorism. On the contrary, it signals the true beginning of that debate.

Which groups pose a sufficient threat to U.S. national security to warrant the use of military force, aside from al Qaeda? When is military detention proper, aside from the context of persons captured in relatively traditional combat scenarios? When should Northern Command rather than the FBI take action domestically? These are just a few of the immensely difficult questions that lie beyond the scope of the new consensus. Each reflects the fact that other instruments of national power aside from military mechanisms remain critical to counterterrorism policy. The 9/11 Commission Report correctly observes that "long-term success" against terrorism "demands the use of all elements of national power," including not just military force but also "diplomacy, intelligence, covert action, law enforcement, economic policy, foreign aid, public diplomacy, and homeland defense." This is precisely the view stated by the President in his landmark address to Congress on September 20, 2001, and it too must become an accepted part of the emerging bipartisan consensus.

Unfortunately, discussions of counterterrorism policy all too often portray it as a zero-sum game in which decision-makers must view terrorists either through the lens of war or through the lens of law enforcement, diplomacy, and the like, but not both. This is a false choice, and we must take care that the language of the war on terrorism does not have the effect of reinforcing such perceptions. Good counterterrorism policy can and must make simultaneous use of all the levers of national power, at times favoring one approach over another in light of best assessment of the balance of long- and short-term costs and benefits. We are vastly better off today because of our use of military force in Afghanistan, but it does not follow that military force is the best choice for all subsequent circumstances that arise.

Secretary of Defense Rumsfeld made this point in vivid fashion in an October 2003 memorandum he sent to General Richard Myers, Chairman of the Joint Chiefs of Staff, General Peter Pace, Vice-Chairman of the Joint Chiefs, Deputy Secretary of Defense Paul Wolfowitz, and Under Secretary of Defense for Policy Douglas Feith on the subject of the "Global War on Terrorism." The memo raised the fundamental question whether we are winning or losing this conflict. And that question, Rumsfeld wrote, boiled down to the following: "Are we capturing, killing or deterring and dissuading more terrorists every day than the madrassas and the radical clerics are recruiting, training, and deploying against us?"

This formula captures the dilemma inherent in the war on terrorism. On one hand, military force in many instances will provide the most effective means of killing or incapacitating terrorists. On the other hand, in some circumstances the use of military force may entail offsetting costs (such as increased recruitment and support for terrorism) that outweigh these benefits. No one-size-fits-all approach is possible. Where non-military options have proven to be toothless, as was the case in Afghanistan, the calculation in favor of military force will be relatively easy to make. In other contexts the call will be more difficult, but sound policymaking demands that we at least make the attempt. With luck, this approach to counterterrorism policy too will become a component of the post-9/11 consensus.

Robert M. Chesney, assistant professor of law at Wake Forest University School of Law, is an officer of the Section on National Security Law of the Association of American Law Schools and writes frequently about terrorism. Comments and criticisms are always welcome at rchesney@law.wfu.edu.

Intelligence Community Reform in Congress

In response to the findings of the bipartisan National Commission on Terrorist Attacks Upon the United States, more commonly known as the 9-11 Commission, the House of Representatives and Senate each have passed separate bills to implement the Commission's recommendations.

Both the House and Senate bills contain some of the most significant intelligence reforms in 50 years. Incorporated in each bill are several areas of intelligence reform, most notably including the creation of a National Intelligence Director and a Counterterrorism Center, information sharing, congressional oversight, financing, and national preparedness.

In spite of the passage of the bills, deep fissures still remain among Republicans and Democrats. Differences also exist amongst moderate and conservative Republicans as to the parameters that should define the debate regarding intelligence reform. After the House received the Senate's final version on October 16, it is apparent that there are also clear distinctions between the Senate and the House's vision of intelligence reform.

House Intelligence Reform - H.R. 10

The House of Representatives passed its own intelligence reform legislation, the "9/11 Recommendation Implementation Act," (H.R. 10) by a 292 to 134 vote on October 8, 2004. Despite persistent entreaties from their Senate counterparts, House Democrats, and families of September 11th victims to produce a bill closely aligned with the Senate version, the House Republican leadership pushed through a measure which requires drastic compromises if Congress is to make good on its promise to reform the intelligence system this year.

While the House bill is in agreement with its Senate counterpart in establishing a National Intelligence Director and a National Counterterrorism Center, the House bill is packed full of additional measures which many House Republican moderates and most Democrats have criticized as being irrelevant to intelligence reform while greatly increasing the overall cost of the legislation.

Several of the most contentious non-intelligence provisions include:

- the creation of national standards for issuing driver's licenses;
- an increase in the number of border patrol officers and immigration agents;
- greater powers for law enforcement authorities to use surveillance on individuals affiliated with terrorist groups but who are suspected of operating as "lone wolf" operatives;
- the empowering of the government to deport non-U.S. citizens suspected of having ties to terrorist organizations or countries known to practice torture against detainees without having been tried or convicted of any crime in the United States; and
- expediting the deportation of any immigrant suspected of having entered the country illegally within the last five years.

Senate Intelligence Reform – S.2845

The Senate was the first to pass its version of the reform legislation (S. 2845) on October 6th by a vote of 96 to 2. The "National Intelligence Reform Act," also known as the Collins-Lieberman bill, after its two main sponsors, Government Reform Committee Chairwoman Susan Collins and Ranking Member Joseph Lieberman, follows the recommendations of the 9/11 Commission more closely than the House bill and has been endorsed by Chairman Thomas Kean and Vice Chairman Lee Hamilton. The bill incorporates 39 of the 41 intelligence reform recommendations made by the 9/11 Commission in its final report. These reforms include the shifting of significant budgetary authority away from the Pentagon.

The Senate legislation includes the following reforms to the United States intelligence system:

- creation of the National Intelligence Director (NID) position to advise the President on intelligence matters affecting national security, and to manage the National Intelligence Program which includes the CIA, the National Security Agency, National Geospatial-Intelligence Agency and National Reconnaissance Office, the FBI's Intelligence office, and the Department of Homeland Security's information analysis function;
- creation of the National Counterterrorism Center (NCC), also managed by the NID, which is designed to "unify" and "integrate" information gathering and analysis operations for U.S. civilian and military counterterrorism intelligence at home and abroad;
- establishment of a Joint Intelligence Community Council (a Joint Chiefs of Staff for the intelligence community) to assist the Director in implementing a "unified national intelligence effort";
- directs the President to establish an information sharing network to promote the sharing of intelligence and homeland security among federal, state and local law enforcement authorities and relevant private sector entities;
- integration of all security clearance investigations into a single agency to streamline and expedite the processing of clearance applications;

Continued on page 8

National Security Agenda

In October, both houses of Congress moved to complete their legislative agendas prior to the November election. The House and Senate are set to reconvene for legislative business on November 16, 2004. Before departing for their home districts, several key pieces of national security legislation were passed.

HR 4567 Department of Homeland Security Appropriations Act for 2005

The purpose of this Act is to allocate the federal budget for the Department of Homeland Security and set spending priorities for 2005. There are four key provisions of this Act. First, the Act provides funding for the U.S. Visitor and Immigrant Status Indicator Technology project. Designed to improve border control and immigration, the project seeks to gather into one system information about visitors to the United States, in order to determine status for admission and appropriate benefits. The project is authorized by the Illegal Immigration Reform and Immigration Responsibility Act of 1996. Second, to assist state and local governments with terrorism prevention, the Act allocates in excess of $3 billion to be disbursed through formula-based grants, law enforcement terrorism prevention grants, and discretionary grant programs. Third, the Act directs the Secretary of the Department of Homeland Security to create and implement an effective system for air cargo inspection and screening on passenger aircrafts. Fourth, the Act allocates budgets for the Transportation Security Administration, U.S. Coast Guard, U.S. Secret Service and Federal Air Marshals.

The Senate passed the bill on September 14, 2004 and the House passed the final conference report on October 13, 2004. The President signed the bill into law on October 18, 2004.

HR 4200 Defense Authorization Act for 2005

House and Senate conferees reached agreement on October 8, 2004 for a defense budget of $445.6 billion for fiscal year 2005. The budget includes expenses for the Department of Defense and national security programs of the Department of Energy. This year's authorization is focused on critical military force protection resources to provide our men and women in uniform with effective defense from new and developing threats. New infantry equipment, improved surveillance, and equipment against Improvised Explosive Devices lead the list of expenditures. The bill also sets out $572 million for Up-Armor Humvees, $100 million for Vehicle Add-On Armor Kits, $12.6 million for Medium Tactical Vehicle Development that provides combat support in the field, $8.1 million for Assault Breacher Vehicles that operate in minefield and areas with complex obstacles, and $51.5 million for Bradley Fighting Vehicles that transport and operate as a shield for troops on the battlefield. The bill also authorizes $1.45 billion in support of the chemical and biological defense programs designed to protect troops and civilians.

On October 9, 2004, the House and Senate passed the conference report. The House approved the report 359-14, while the Senate approved it by unanimous consent. The bill was cleared for the White House on October 9, 2004.

For complete text of these bills, please visit http://thomas.loc.gov.

Written by Margaret Lee Wood, a student at Catholic University Columbus School of Law.

Intelligence Community Reform

Continued from page 7

- discloses information about the nation's intelligence budget; and
- creation of a database to allow anti-terrorism agencies to access commercial and law enforcement records.

The Intelligence Reform Debate
The Democratic Dilemma

The initial passage of the House and Senate bills has aroused criticism from Democratic members. Many House Democrats are concerned that the aforementioned contentious reforms will encroach on civil liberties in several ways. Democrats argue that that the House bill strays far from the 9-11 Commission recommendations to strengthen the protection of civil liberties by ignoring the Commission's recommendation to create a "watchdog board" to prevent civil liberties abuses. Democrats also contend that the House bill unfairly expands the PATRIOT Act in many respects, including: allowing employers easier access to arrest records; easing prosecution of individuals involved with groups that the government deems "terrorist organizations" even if the person has not given any money to the group and has not participated in violent activity; infringing upon personal privacy by creating the national identification card system; and placing unnecessary restrictions on the immigration system, including expediting the deportation of immigrants to nations where they will be tortured.

There are fewer reservations among Democrats concerning the Senate bill because it more closely follows the 9/11 Commission's recommendations. Nonetheless, Democrats have expressed serious concerns regarding the Senate proposal to allow the collection of information on Americans without probable cause. They argue that government agents will be able to invade law-abiding citizens' privacy with little legal obstruction.

The Republican Dilemma

As the House begins reconciling its bill with that of the Senate, conservative Republicans continue to argue that neither the House nor Senate proposals effectively target the most serious weaknesses within the intelligence infrastructure. The Republican-led Congress chose to wait until after the election to pass the legislation. Congress now has two broad options:

- Congress can pass meaningful and lasting reform which permanently shifts institutional allegiances and powers within the legislative and executive branches and alienates key committee chairmen;
- Congress can pass a watered down final bill which greatly limits the budgetary and decision-making authority of the National Intelligence Director and provides House leadership with costly non-intelligence-related provisions.

Whichever strategy prevails, Republican leadership believes that the best hope for seeing a final passage of the current reform proposals lies in hammering out the substantive differences between the two packages during closed-door Conference committee sessions.

Written by Ben Davis and Catherine Slattery. Davis and Slattery are students at Catholic University Columbus School of Law.

PATRIOT Act. . .

Continued from page 2

Amendment. The *Miller* decision prompted Congress to enact the Right to Financial Privacy Act (RFPA) in 1978. In broad terms, the RFPA created statutory protection for the records that the *Miller* Court found were beyond the reach of the Fourth Amendment. Congress included an exception for foreign intelligence investigations, allowing requests for protected information by government authorities who were "authorized to conduct foreign counter- or foreign positive-intelligence activities for purposes of conducting such activities" to be honored without notice to the targeted customers. Since just two years had passed since the Church and Pike Committees had completed their work, Congress remained wary of counterintelligence, and it noted that the exception should "be used only for legitimate foreign intelligence investigations; investigations proceeding only under the rubric of 'national security' do not qualify."

By the mid-1980s, the FBI had begun to push for authority to compel the production of financial records in counterintelligence matters without a judicial order. The existing RFPA language allowed the FBI (and other counterintelligence agencies) to make requests for information, but it did not require financial institutions to comply. The FBI argued that while most institutions did comply, a significant number did not, often citing the constraints of state constitutions or banking privacy laws. The congressional response was to give the FBI specific authority to compel the production of financial records using a "national security letter."

In granting compulsory process to FBI counterintelligence in 1986, Congress created a new, hybrid legal standard: "specific and articulable facts giving reason to believe" that the targeted person is an "agent of a foreign power." The "agent of a foreign power" criterion was not new; it had been established in FISA as a way to identify proper subjects of counterintelligence electronic surveillance. The innovation was in the quantum of proof required: "specific and articulable facts giving reason to believe." The Conference Report noted that the standard was "significantly less stringent

Continued next page

PATRIOT Act. . .

Continued from page 2

than the requirement of 'probable cause,'" and it indicated that the "reason to believe" standard should "take into account the facts and circumstances that a prudent investigator would consider insofar as they provide an objective, factual basis for the determination." An earlier report indicated that the House considered the higher standard of "probable cause" inappropriate, given the holding in *Miller*.

Shortly before Congress modified the RFPA to provide national security letter authority, it enacted the Electronic Communications Privacy Act (ECPA). ECPA broadly updated the law governing electronic communications by refining prohibitions on their interception, extending legal protections for traditional telephone service to include all wire and electronic communications services, and regulating stored wire and electronic communications. ECPA attempted to keep pace with evolving technology by extending statutory protection to electronic and wire communications stored by third parties (for example, on the servers of an Internet service provider or corporate network) and to electronic communication transactional records. The Act also restricted the government's access to live telephone transactional data (commonly known as "pen register" and "trap and trace" data), requiring it to obtain a court order based upon a certification of relevance to an ongoing criminal investigation. Like the RFPA, ECPA contained a special provision for counterintelligence access, and the exception was broadened by a 1993 amendment.

The final type of national security letter emerged in 1995, when the FBI sought counterintelligence access to credit records. The FBI stated that RFPA national security letters had proven very useful, but that counterintelligence agents still had to employ intrusive or time-consuming techniques (physical and electronic surveillance, mail covers, and canvassing of local banks) simply to determine where targeted individuals maintained accounts. The same information was readily available from credit bureaus and was commonly obtained in criminal investigations through the use of a subpoena. Congress's response was to amend the Fair Credit Reporting Act (FCRA) by giving the FBI national security letter authority to obtain certain information from credit reporting agencies. The authority essentially replicated that granted in the 1993 ECPA amendment, employing the same legal standard: "necessary for the conduct of an authorized foreign counterintelligence investigation" and "specific and articulable facts" giving reason to believe the target was (or was in contact with) an agent of a foreign power. Similarly, the new FCRA provision embodied two levels of access to information: if the target was an agent of a foreign power, the FBI could get the identity of all financial institutions at which the target maintained an account; if the target was merely in contact with an agent of a foreign power, the FBI got "identifying information" limited to "name, address, former addresses, places of employment, or former places of employment."

In addition to the national security letter authorities just described, in a 1998 amendment to FISA the FBI acquired two new tools to collect transactional information. The amendment for the first time permitted "pen register" and "trap and trace" authorization to be obtained through the FISA process. The FISA amendment also created procedures for emergency use of the authority, certain restrictions on the use of information obtained through the authority, and a notification and challenge procedure triggered when information obtained is used in a subsequent proceeding. The notification and challenge procedure mirrors those found elsewhere in FISA for electronic surveillance and physical searches.

The 1998 amendment to FISA also created the direct antecedent of §215 of the USA PATRIOT Act. It allowed the FBI to seek a FISA court order compelling the production of business records from common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities. The standard was set at the now-familiar "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or agent of a foreign power." Like the new pen register authority and all of the existing national security letter authorities, this provision imposed a non-disclosure requirement on the recipients of the court order. There is almost no legislative history for these two new provisions.

In summary, on the eve of the September 11 terrorist attacks

Continued next page

Advisory Committee. . .

Continued from page 1

Vliet, and **Lynne Zusman.** We look forward to welcoming them into our 'alumni group.'

The Standing Committee also benefits from the contributions made by our prestigious group of Counselors. They include: **Judge Robinson Everett,** Founder, Center on Law, Ethics and National Security at Duke University School of Law; **Ambassador Max Kampelman,** former Delegation Head to the Nuclear and Space Arms Negotiations in Geneva; **John O. Marsh,** former Secretary of the Army and former Congressman; **Professor John Norton Moore,** University of Virginia School of Law and Director of the Center for National Security Law at UVA, **Judge William Webster,** former Director of the FBI and former Director of Central Intelligence; and **R. James Woolsey,** former Director of Central Intelligence.

PATRIOT Act. . .

Continued from page 9

the FBI had five separate legal authorities that addressed the need to compel production of transactional information in counterintelligence investigations: three types of national security letters (under RFPA, ECPA, and FCRA), the FISA pen register/trap and trace authority, and the FISA business records authority. All of these authorities specified the types of records that could be obtained, and all the records specified were, according to the reasoning of the Supreme Court in *Miller*, outside the protection of the Fourth Amendment. All of the authorities required, in essence, that the information sought be relevant to an authorized counterintelligence investigation and that the FBI demonstrate "specific and articulable facts giving reason to believe" that the investigative targets were foreign powers or agents thereof.

Section 215 of the USA PATRIOT Act

The USA PATRIOT Act revisions to authorities governing counterintelligence access to transactional information are spread across three sections: §214 ("Pen register and trap and trace authority under FISA"), §215 ("Access to records and other items under the Foreign Intelligence Surveillance Act"), and §505 ("Miscellaneous national security authorities"). The cumulative effect of these three sections is to make an across-the-board adjustment of the legal standard for access from "relevance" plus "specific and articulable facts giving reason to believe" the target was a foreign power or an agent of one, to simple "relevance" to an investigation to protect against international terrorism or clandestine intelligence activities (provided such an investigation of a U.S. person is not based solely on protected First Amendment activity).

Of the various revisions, those in §215 go farthest, replacing the old "business records" authority in Title V of FISA. While the old language allowed the FBI to seek "an order authorizing a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility to release records in its possession," the new section allows an order requiring the production of "any tangible things (including books, records, papers, documents, and other items)." The new language, like the new national security letter language, includes the caveat that the material sought must be "for an 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." Unfortunately, there is very little in the way of legislative history for §215.

Public criticism of the USA PATRIOT Act began almost immediately, with expressions of concern over the speed with which the legislation was produced and the lack of public hearings. Some members of Congress suggested that the Administration, and particularly the Attorney General, were exploiting the chaotic post-9/11 environment to accomplish a dramatic expansion of executive branch authority. Although criticism of the Act in general, and of §215 in particular, has proliferated since passage, the key issues remain three first identified in the Senate debates: (1) §215 violates the Fourth Amendment and/or various statutory protections because it allows the government to compel production of personal information without a showing of probable cause; (2) §215 is impermissibly broad, in that it allows the FBI access to information about innocent third parties upon a showing of mere relevance to an investigation; and (3) there is no effective oversight of the use of §215.

Library records have emerged as the most prominent example cited in support of the first criticism, since government access to these "tangible things" seems to raise state law, First Amendment, and Fourth Amendment issues. Library and bookseller associations are probably now the most aggressive opponents of §215, with the libraries motivated, in part, by their historical experience with FBI counterintelligence operations. Not all of their legal arguments withstand a closer look, however. For example, the claim that library patron records are protected by the Fourth Amendment is not convincing. Rather, library patron records fall squarely into the category identified in *United States v. Miller*, that is, information that ceases to be a person's "private papers" by virtue of its being handed over to a third party who may convey it to the government. The Justice Department certainly espoused this view, arguing that "any right of privacy possessed by library and bookstore patrons in such information is necessarily and inherently limited since, by the nature of these transactions, the patron is reposing that information in the library or bookstore and assumes the risk that the entity may disclose it to another." Indeed, this same view was expressed in the congressional debate on the USA PATRIOT Act.

The controversy over library records might not be nearly so acrimonious if it were clear that the names of borrowers could somehow be separated from the titles (and by inference from the contents) of the books they borrow. Such anonymization of personal reading habits might be required if §215 provided access only to transactional information, that is, information that documents transactions without necessarily revealing the substance of those transactions. Given that §215 was clearly part of a set of parallel revisions to all FBI counterintelligence authorities for access to transactional information (national security letters, pen register/trap and trace, and business records), it seems reasonable to conclude that Congress saw §215 as applying only to transactional information that is not subject to constitutional protections. The limitation of §215 to transactional records also would be consistent with the historical development of FBI counterintelligence authorities sketched out above.

Whatever the intention of Congress or the understanding of the executive branch, however, the language of §215 contains no limitation, creating confusion. The FBI, for example, notes

the uncertain scope of §215 (and the problem of library records) in its legal instructions to FBI agents on the use of §215 authority. In this respect, §215 parts company with the other "transactional" counterintelligence authorities, all of which specify the data to which they apply, either explicitly or by their incorporation into the very statutes that protect the information at issue.

The second major criticism of §215 concerns the movement from the standard of "specific and articulable facts giving reason to believe" that the target is an agent of a foreign power to a standard of "relevance to an authorized investigation to protect against international terrorism or clandestine intelligence activities." Critics charge that this change gives the FBI too much authority, allowing the Bureau to conduct "fishing expeditions" by seeking the records of people who are not actual targets of an investigation. Some of these critics illustrate their point with hypotheticals based on imagined applications of the section.

It is undeniable, of course, that the USA PATRIOT Act lowered the standards for counterintelligence collections. This change was carefully considered, however, and apparently it was influenced by the FBI's identification of examples from actual operations. Even Senator Patrick Leahy, who is generally suspicious of expanded FBI authorities, found that the "FBI has made a clear case that a relevance standard is appropriate for counterintelligence and counterterrorism investigations, as well as for criminal investigations." Other members echoed the idea that counterintelligence agents pursuing terrorists should have tools at least as readily available as those open to criminal investigators.

The third major criticism of §215 is that it lacks effective oversight for the exercise of such an expansive power, in the form of judicial approval, executive branch or congressional review, or notice to surveillance targets. Critics claim that although exercise of the power requires a court order, the judge has no meaningful discretion in considering a §215 application. While the plain language of §215 directs the judge to issue the business records order if the judge finds "that the application meets the requirements" of the section, the only "requirement" (aside from making the application to a FISA judge or a specially designated magistrate) is that the application specify that "the records concerned are sought for an authorized investigation." The language describing the judge's role is essentially the same as that found in FISA's pen register/trap and trace provisions (both the pre- and post-USA PATRIOT Act versions), which appear to be derived from the criminal pen register statute. The Justice Department has made statements implying that the court does exercise some discretion, but it points to no support for this proposition. In the context of criminal pen registers, the Tenth Circuit Court of Appeals has found that the limited judicial review of a pen register request does not render the statute unconstitutional. The Court recognized, but did not decide, the question of whether, despite the language of the statute, the reviewing court could inquire into "the government's factual basis for believing" that the request is relevant. The criticism of §215 on this point remains valid: the practical nature of the FISA court judge's review of a business records application remains uncertain, as does the propriety of the standard of review, in light of the broad scope of §215 authority.

Secrecy has been recognized as essential since the very beginning of American intelligence operations. In many respects, the regulatory scheme governing counterintelligence, the higher legal standards for counterintelligence authorities, and even the "wall" separating intelligence and criminal law enforcement have all functioned to counter-balance and contain a tendency toward excessive secrecy in this area. The USA PATRIOT Act alters some of these constraints by lowering the legal standards for transactional information authorities and by largely dismantling the "wall." It should certainly prompt a re-examination of some secrecy provisions. However, the operational and policy concerns that consistently tipped the balance in favor of secrecy, even during the counterintelligence reforms of the 1970s, are even more pressing in the post-9/11 environment.

My goal in this discussion has not been to defend §215 against its critics, but rather to place those criticisms within the larger context of the counterintelligence legal authorities and the evolution of access to transactional information.

Revising Section 215

Within the next year, Congress will have to decide whether or not to retain §215 (along with other parts of the USA PATRIOT Act) in its present form. The sunset clause of the Act was intended to give Congress a chance to re-evaluate the necessity of these expanded authorities. In the case of §215, it appears that Congress will have very little operational data upon which to base its decision. The FBI and Justice Department will doubtless continue to insist that the capability provided by §215 is necessary, even if it is rarely employed. Critics of the Act will argue that the potential for abuse is so great that it should be eliminated or severely curtailed. Both sides begin from sound premises. The nature of the terrorist threat demands that our counterintelligence legal tools be effective, flexible, and readily available. However, these tools also represent compulsory, secret government access to personal information, and therefore they should be available only under conditions that minimize their potential for abuse.

I suggest that by drawing from the evolution of these tools and other counterintelligence authorities over time, §215 can be revised to accommodate the concerns of both sides. I make two assumptions in proposing these revisions. First, I assume that the FBI will continue to have an actual need for the general capability to compel production of transactional information, beyond that already provided for in national security letter and FISA pen register authorities. My second assumption is that the §215 business records authority rarely will be used. If the authority is properly limited to

Continued next page

PATRIOT Act. . .

Continued from page 11

transactional information, there should not be frequent occasions to invoke it. The most useful, and therefore frequently sought, types of transactional information are already available to the FBI through the more accessible national security letter authorities. A great deal of the remaining transactional information is subject to no legal protection at all, and it can be provided voluntarily. The compulsory authority will therefore be used only when the operation of some other law, concern over civil liability, or the resistance of the records custodian prevents voluntary production. Since that authority likely will be used infrequently, creation of a more demanding process for the government could be assumed to have a relatively minor impact on operations.

My first revision to the business records authority would be to limit its application to transactional records that are truly relevant to authorized investigations. This could be accomplished by amending §215 to require (1) that each application recite facts demonstrating that the records concerned are sought for an authorized investigation; (2) that no application be approved unless the FISA judge finds that the records are relevant to a proper investigation; and (3) that no application be approved unless the judge determines that the records sought are not subject to the protection of the Fourth Amendment, and are not otherwise protected from disclosure to the FBI by federal law.

This amendment would improve the statute in several ways. First, it would restrict the application of the authority to genuinely transactional records. Second, it would establish the authority of the FISA judge considering an application to assure compliance with the legal standard. Finally, the language would accommodate other statutes controlling the privacy of particular types of information. Should Congress decide to protect library records specifically, or to give such treatment to some other body of transactional information, the business records authority could continue to function. This change would alleviate concerns over the scope of the authority and over the expansiveness of the relevance standard. The court would be in a position to detect and terminate unwarranted "fishing expeditions." Decisions of the FISA judge on these applications would be subject to review by the Foreign Intelligence Surveillance Court of Review, thus allowing further refinement of the legal standard.

My second revision would address the question of notice to the person to whom the information pertains. While the counterintelligence value of the authority would vanish if notice were commonly required, there is precedent for giving the affected person notice when the government uses the information for a purpose other than counterintelligence. The other three FISA-based counterintelligence authorities (electronic surveillance, physical search, and pen register/trap and trace) all impose restrictions on the use and dissemination of information gained through the FISA authority, requiring notice to the person affected if the government intends to "enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States" information so obtained, and giving the aggrieved party a specific procedure through which to challenge the use of the information in a criminal proceeding. The text of these provisions could easily be inserted into the business records section, with the phrase "business records order" replacing the phrase "pen register or trap and trace device" throughout. This change would defuse some of the criticism over notice, and it would allow for the development of additional case law as application of the authority was examined in the criminal courts.

These two revisions, if adopted, would place §215 more firmly in the tradition of carefully circumscribed counterintelligence authorities. Like national security letters and the FISA pen register authority, the scope of §215 authority would then be defined as limited to transactional materials. The definition would, of course, be dynamic, shaped by the action of the courts. The authority therefore could remain flexible, while concerns about its application to protected data would be soothed. The revisions would also maintain the principle that the use of counterintelligence authorities calls for greater control than does application of analogous criminal investigatory approaches. The revised authority would function at roughly the legal standard of the grand jury subpoena, but with direct, rather than indirect, judicial oversight.

The changes proposed in this article, or something like them, are essential if Congress chooses to retain §215. The law as written simply does not inspire sufficient confidence to overcome the fear of abuse. During the congressional debates on the USA PATRIOT Act, there was extensive quotation of revered patriots, led by a warning attributed to Benjamin Franklin that "if we surrender our liberty in the name of security, we shall have neither." Franklin's actual words are more nuanced and present a more direct challenge to §215 in its present form: "Those who would give up essential Liberty, to purchase a little temporary safety, deserve neither Liberty nor Safety." Careful attention to the actual history of counterintelligence authorities, arcane and inaccessible though it may be, will yield the raw materials needed to construct an effective, balanced authority to replace the current §215. An appropriate narrowing of the statute will both protect what is essential to our freedoms and enhance our long-term security.

Michael J. Woods is a former chief of the FBI's National Security Law Unit and later served as Principal Legal Advisor to the National Counterintelligence Executive. The views expressed in this article are his own and do not necessarily reflect the position of any U.S. government component.