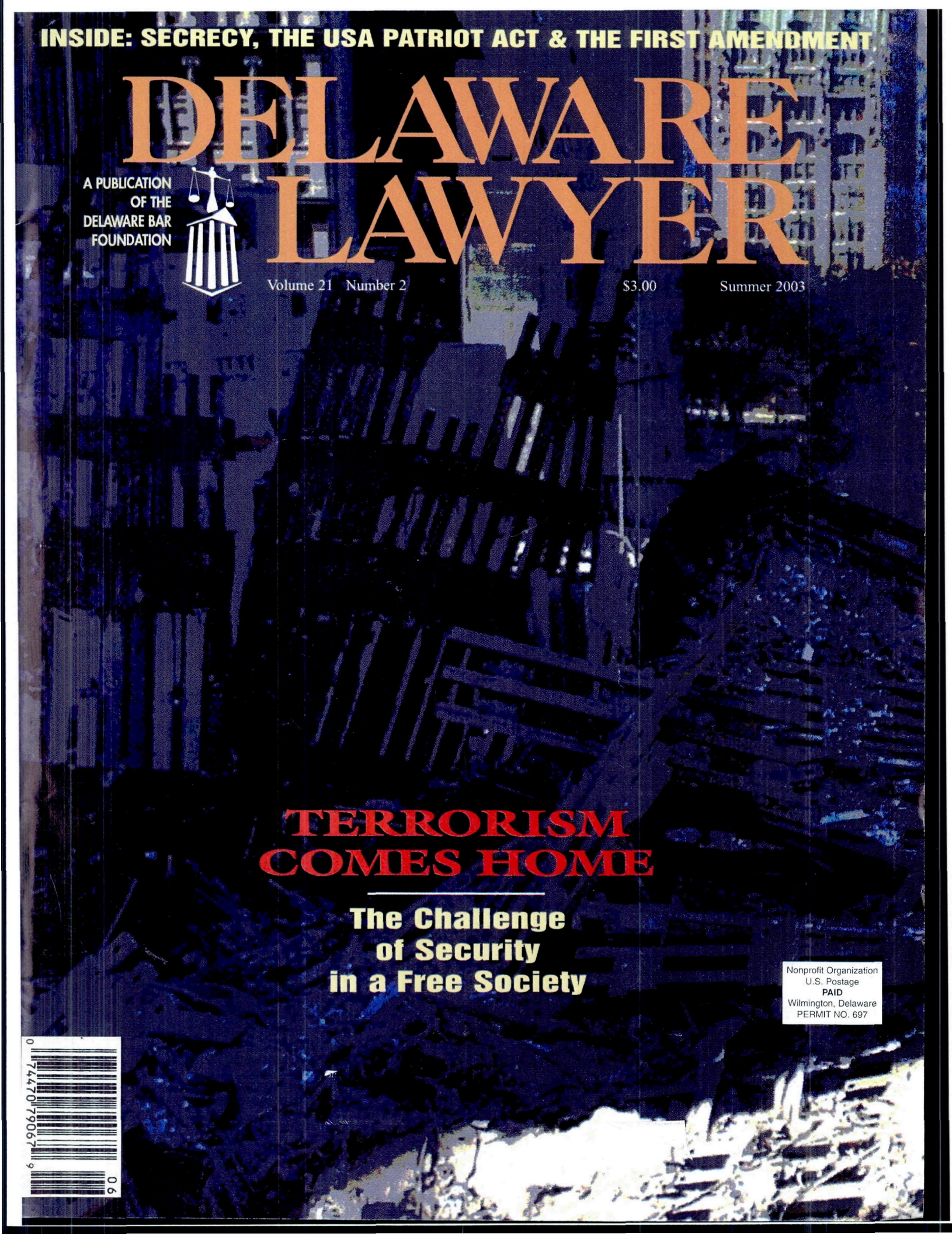
INSIDE: SECRECY, THE USA PATRIOT ACT & THE FIRST AMENDMENT

DELAWARE LAWYER

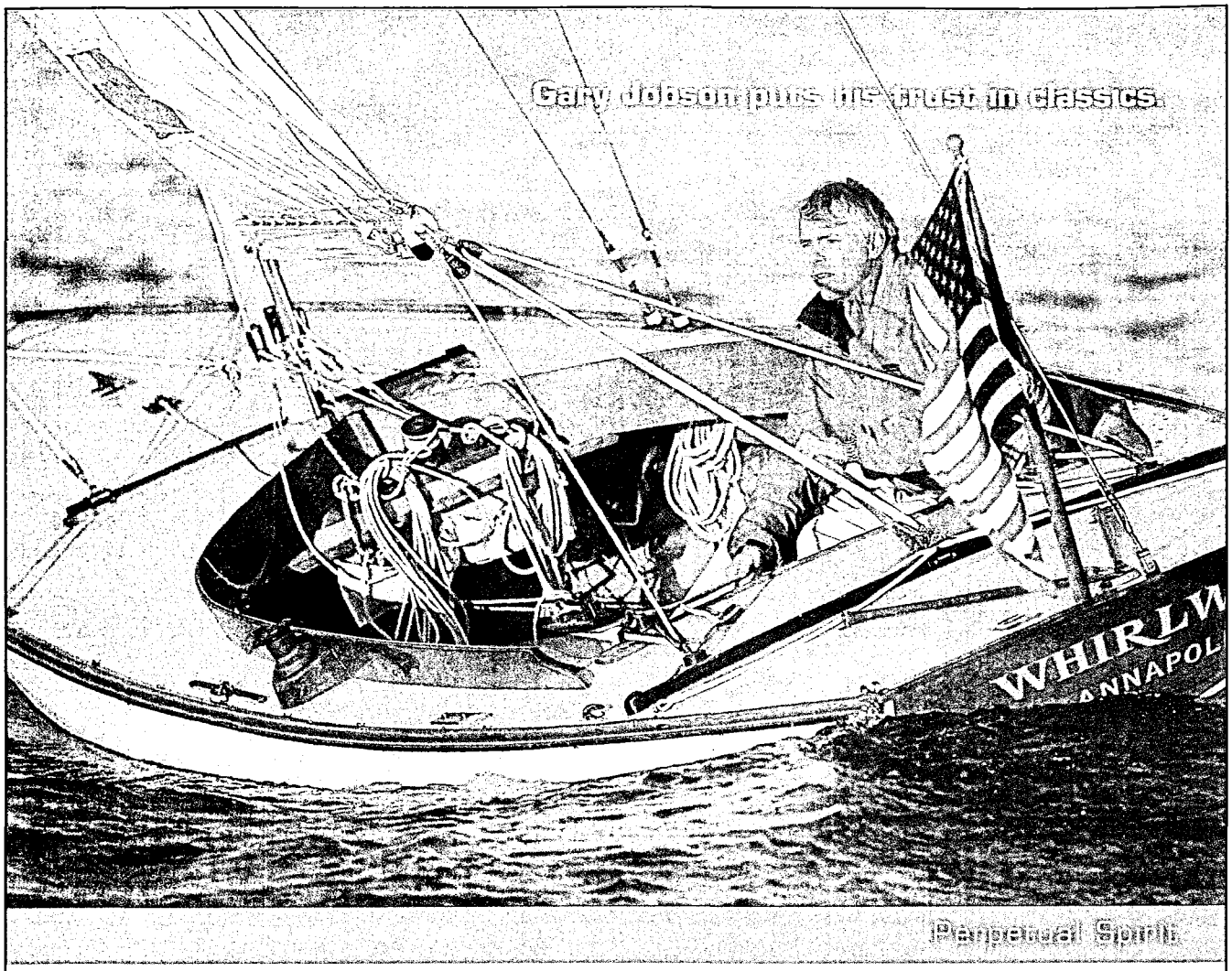
A PUBLICATION OF THE DELAWARE BAR FOUNDATION

Volume 21 Number 2 $3.00 Summer 2003



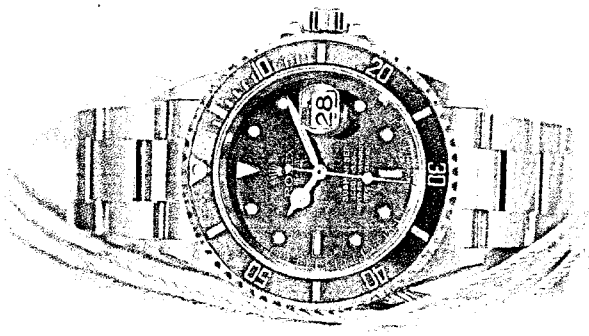
TERRORISM COMES HOME

The Challenge of Security in a Free Society



Having competed successfully in a variety of boats, Gary Jobson's choice for himself is a classic Herreshoff 28-footer, whose graceful design will never go out of style. The same aesthetic is reflected in his timepiece.

ROLEX



Rolex Oyster Perpetual Submariner in stainless steel and 18kt gold.
Officially Certified Swiss Chronometer.

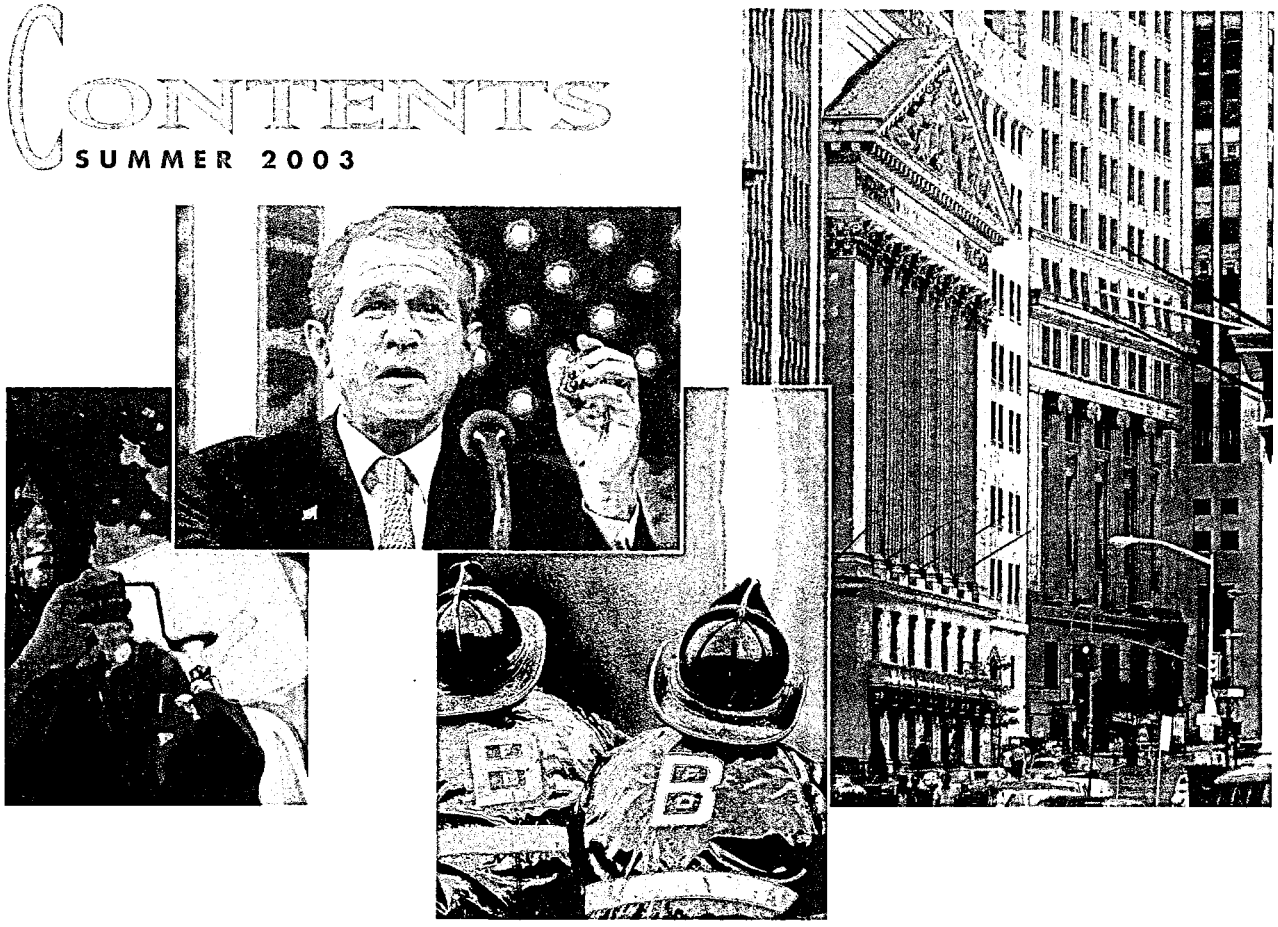
Carl DOUBÉT Jr.

JEWELERS

3801 KENNETT PIKE, GREENVILLE CENTER, GREENVILLE, DELAWARE (302) 888-2991

CONTENTS

SUMMER 2003



After the tragic and senseless attack on the World Trade Center and the Pentagon, the United States government launched a series of initiatives to prevent future such attacks and to bring al-Qaeda conspirators to justice. Several of these actions were and continue to be controversial. The USA Patriot Act increased the government's authority to investigate, intercept communications, and detain suspected terrorists and curtail their sources of funding. Many of these powers may well have been necessary, yet there is concern that the reach of this new authority may have been overly broad and inconsistent with fundamental constitutional principles. The United States government invaded Afghanistan overthrowing the Taliban government that had provided safe harbor to al-Qaeda and then attacked Iraq deposing Saddham Hussein and the Baathist party.

Our contributors address these controversial decisions from several different perspectives. Cynthia Ryan, Chief Counsel of the Drug Enforcement Administration, explains the purposes of the USA Patriot Act and addresses the benefits of Title II expanding the coverage of the federal electronic surveillance statutes to provide additional tools for law enforcement. Michael Kelsey examines the many changes to the anti-money laundering statutes contained in the Patriot Act and provides practical advice for the private practitioner. Drew Fennell of the ACLU raises several civil liberties concerns about the government's increased powers of surveillance over U.S. citizens and non-citizens alike. Professor Erin Daly examines the broader implications of the Patriot Act for freedom of speech and expression fundamental to our society. In my contribution, I examine the international legality of the U.S. attacks on Afghanistan and Iraq both under traditional international legal doctrine on the use of force and wider alternative approaches to justify these actions.

Each of the articles grapples with a fundamental conundrum of our times—how to permit necessary actions to prevent terrorism while placing limits on government actions in order to cabin abuse and preserve essential freedoms.

J. Patrick Kelly

ERIN DALY

Erin Daly is Professor of Law at Widener University School of Law and has served as Director of Widener's summer program in Sydney, Australia. Professor Daly (J.D., University of Michigan; B.A., Wesleyan University) practiced First Amendment and employment law at Cooper, White & Cooper in San Francisco from 1990-93. She is admitted to practice in California, and she teaches and writes in the areas of Constitutional Law, Federal Courts, and Comparative Law. She has served as Vice-Chair of the Young Lawyer's Division Law and Media Committee of the American Bar Association.

DREW FENNELL

Drewry Nash Fennell is the Executive Director of the American Civil Liberties Union of Delaware. Drew graduated from Rutgers-Camden Law School, and then served as a law clerk for Vice Chancellor Bernard Balick of the Delaware Court of Chancery. Prior to her position with the ACLU, Drew was an attorney in private practice with the firm of Young Conaway Stargatt and Taylor, LLP.

J. PATRICK KELLY

J. Patrick Kelly is Professor of Law at the Widener University School of Law. A University of Delaware and Harvard Law School graduate, Professor Kelly served in several positions at the Federal Trade Commission 1972-1980, including Assistant to the Director of the Bureau of

(Continued on page 5)

DELAWARE LAWYER
A publication of Delaware Bar Foundation
Volume 21, Number 2

DELAWARE LAWYER
Attention: Chair, Board of Editors
c/o Media Two, Inc.
22 W. Pennsylvania Ave., Ste. 305
Towson, MD 21204

Art Director
Samantha Carol Smith

Subscription orders and address changes should be directed to:
Alexis Cooper (302) 656-1809 x247

Requests for information about advertising should be directed to:
Vera Malkowski (410) 879-9606
vera.malkowski@mediatwo.com

DELAWARE LAWYER is published by Delaware Bar Foundation as part of its commitment to publish and distribute addresses, reports, treatises, and other literary works on legal subjects of general interest to Delaware judges, lawyers, and the community at large. As it is one of the objectives of DELAWARE LAWYER to be a forum for the free expression and interchange of ideas, the opinions and positions stated in signed material are those of the authors and not, by the fact of publication, necessarily those of Delaware Bar Foundation or DELAWARE LAWYER. All manuscripts are carefully considered by the Board of Editors. Material accepted for publication becomes the property of Delaware Bar Foundation. Contributing authors are requested and expected to disclose any financial, economic, or professional interests or affiliations that may have influenced positions taken or advocated in the articles. That they have done so is an implied representation by each author.

(Continued from page 3)

Consumer Protection. From 1983 to 1984 he was Counsel to the Subcommittee on Economic Stabilization of the House Banking Committee. Professor Kelly has served as a visiting Fulbright Professor of Law in Uganda, Director and Founder of the Nairobi International Law Institute, and Director of the Sydney International Law Institute. He is a former Chair of the International Law Section of the Delaware Bar Association.

MIKE KELSEY

Mike Kelsey is PNC Financial Group's Director of Retail and Wholesale Bank compliance as well as its corporate Anti-Money Laundering Compliance Officer. He writes and speaks frequently on money laundering matters and spent a week in Latvia last year consulting with government and bank authorities on money laundering policy on a Financial Services Volunteer Corporation project. Mike became a member of the Delaware Bar in 1983 and lives in Wilmington with his wife (Deputy Attorney General Cynthia Kelsey) and two daughters.

CYNTHIA R. RYAN

Cynthia R. Ryan is the Chief Counsel of the U.S. Drug Enforcement Administration. She graduated from the Widener University School of Law in 1979 and practiced as a Deputy Attorney General in the Delaware Attorney General's Office from 1979 to 1985. ◆

Cynthia R. Ryan

THE USA PATRIOT ACT HELPS LAW ENFORCEMENT MEET THE ANTI-TERRORISM CHALLENGE

September 11, 2002 was a defining moment for our country. While it was not the first terrorist attack within the borders of the United States,[1] it was the most devastating. When the smoke cleared, we began to see who and what we were up against. We knew we could not, and would not, let it happen to us again.

What we soon realized is that these terrorist acts were perpetrated by expertly organized, highly coordinated, and well-financed organizations to advance their political agendas. We face non-state enemies that have no sovereign territory of their own but that enjoy support on various levels from other nations. They operate worldwide without the constraints of national borders or legal jurisdictions. They take advantage of legal loopholes.

The tragic events of September 11 quickly forced us to reevaluate our strategy to protect our homeland and our people in a fundamental way. Although the terrorist threat bore little resemblance to traditional crime, we fought the enemy with a traditional law enforcement strategy; i.e. respond to terrorist attacks at home and abroad as a crime, gather evidence, and pursue prosecution of the perpetrators. While this reactive approach has merit and enjoyed some success, it is insufficient by itself to meet the continuing threat, as was borne out by the 1995 prosecution and conviction of Sheik Omar Abdel Rahman as the mastermind of the 1993 World Trade Center bombing. To protect the American people and property, we must detect and prevent terrorist attacks and prosecute, if possible, later.

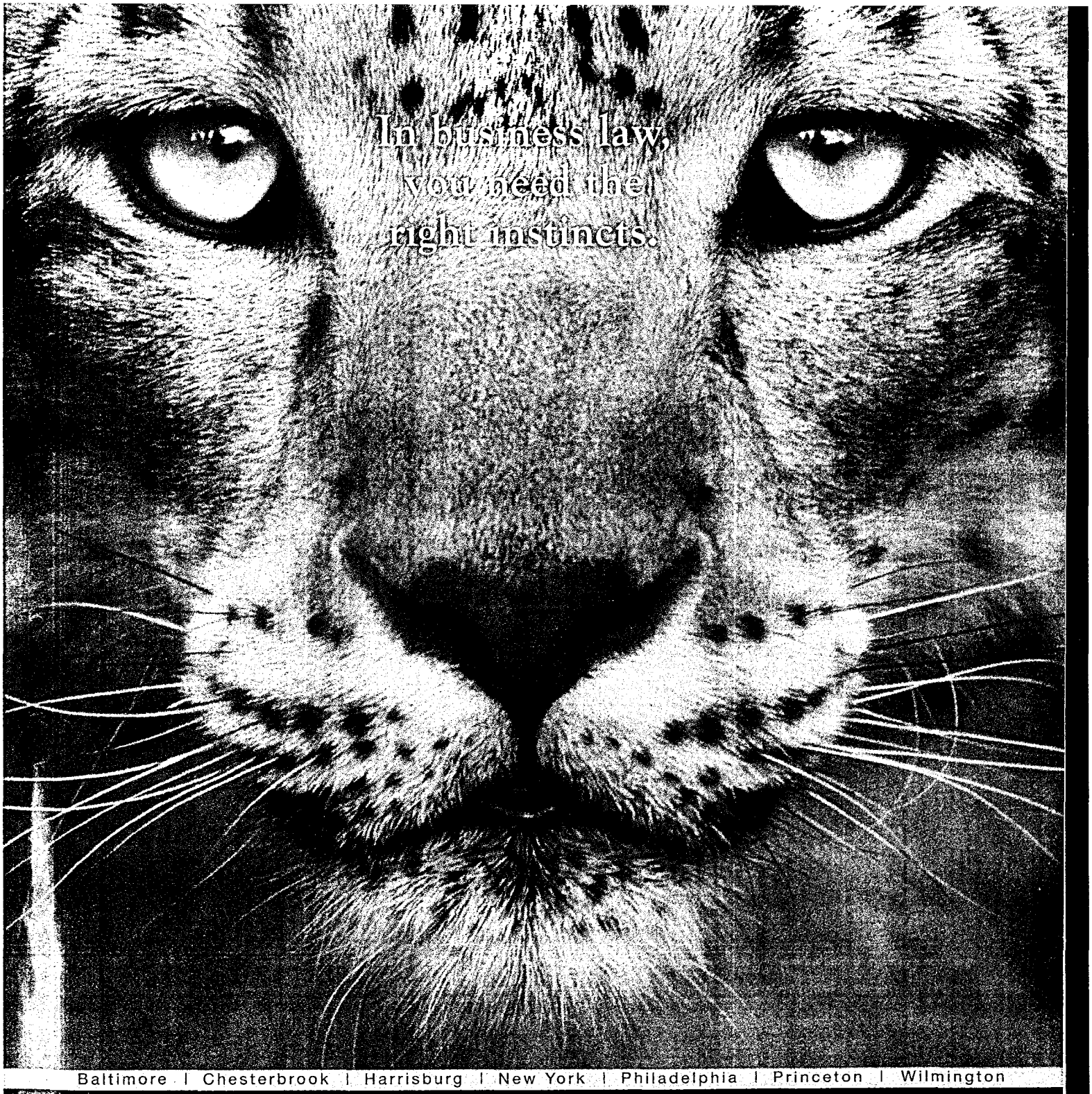
What is the nature of the target in our crosshairs? Our chief terrorist enemy — Al Qaeda — is a disciplined, non-state military-like force. The eleven-volume Al Qaeda terrorist training manual designed for recruits and operatives includes detailed instructions on biological and chemical warfare, assassination and explosives. It is not only intended to be used as an instructional manual, but also as a means of conditioning the mind of the Al Qaeda terrorist to promote violence against its enemies: "the terrorist member 'should have a calm personality that allows him to endure psychological traumas such as those involving bloodshed, murder, arrest, imprisonment, and reverse psychological traumas such as killing one or all of his Organization's comrades.'"[2] Law professor Ruth Wedgwood observed: "At length, the manual instructs new members in countersurveillance, encryption, the preparation of safe houses, and the choice of escape routes after an assassination. The jihad's 'undercover members' are to avoid any outward appearance of 'Islamic orientation.' . . . The hijackers of September 11 who passed through security in the Boston airport looked like ordinary travelers."[3] They are schooled in violence and stealth.

"Terrorist," as defined in the U.S. legal lexicon, is a person who is involved in "violent acts or acts dangerous to human life" in violation of U.S. criminal laws and that "appear to be intended to intimidate or coerce a civilian population, to influence the policy of a government by intimidation or coercion, or to affect the conduct of a government by mass destruction, assassination, or kidnapping."[4] These acts may occur within or outside the territorial jurisdiction of the United States.[5] Essentially, terrorists are violent criminals with a political agenda.

U.S. law enforcement, particularly the Drug Enforcement Administration (DEA), has focused on a specific breed of terrorists — the narco-terrorist.[6] The drugs-to-money-to-terror relationship is historic, but the events of September 11 brought new emphasis to the perennial problem of narco-terrorism. The Taliban, which controlled opium production and directly taxed the drug trade in Afghanistan, welcomed Osama bin Laden and the Al Qaeda organization, which built its financial base with heroin trafficking. While Al Qaeda has used its drug money for the most colossal of terrorist acts, narco-terrorism is more widespread than Al Qaeda. For example, in Colombia the Fuerzas Armada Revolucionarios de Colombia, otherwise known as the FARC, raises its funds, in part, from illicit cocaine trafficking to purchase weapons and finance their attacks on innocent Colombian civilians for its revolutionary cause. In Peru, the Shining Path guerrillas "tax" local drug traffickers to fund their political influence and military force. In Southeast Asia, financial support of the United Wa State Army is primarily derived from heroin and methamphetamine trade.[7]

How do we thwart this global, but very close to home, threat? Our traditional law enforcement approach was not designed to deal with a quasi-military threat such as Al Qaeda. In a recent essay, Abraham D. Sofaer, former Legal Advisor to the State Department, notes that "[a]nti-terrorism efforts must ultimately be judged by whether they prevent attacks which can result in horrendous human and economic consequences" and "[c]riminal prosecution are especially ineffective in deterring fundamentalist terrorist groups."[8]

The attacks on September 11 squarely presented a new challenge for law enforcement. The fight against terrorism can no longer be solely a criminal justice endeavor. We cannot



Baltimore | Chesterbrook | Harrisburg | New York | Philadelphia | Princeton | Wilmington

To understand that no company can prosper by maintaining the status quo, and that thinking ahead is worth its weight in profits. From technology and life sciences to insurance, financial services and more, our in-depth knowledge of specific industries and corporate governance issues makes our attorneys stand out. Our instinct to respond is why our clients rate us far above the competition. In fact, our responsiveness rating is one of the highest ever recorded. Contact us. We think ahead so you can race toward your goals.

SAUL EWING LLP

Thinking ahead.
So you can move ahead.SM

www.saul.com 1-800-355-7777

wait for terrorists to strike to initiate investigations and then take action. We must prevent first, and prosecute second. To prevent, we must be able to detect terrorist activities afoot.

Throughout our nation's history, our laws have constantly evolved to meet new challenges and needs. That different techniques are required to meet a threat to our national security is neither a new nor unconstitutional proposition. Over 30 years ago, for example, the U.S. Supreme Court noted "that domestic security surveillance may involve different policy and practical considerations from the surveillance of 'ordinary crime.'"[9] A recognition that insulated, traditional organized crime required a different approach resulted in the Racketeer Influenced and Corrupt Organizations Act (RICO) in 1970.[10] Subsequently, the threat of sophisticated and violent drug trafficking organizations resulted in a tailored legal approach, a new offense entitled Continuing Criminal Enterprise (CCE).[11] Similarly, the full recognition of the scope and nature of the terrorist threat facing our country resulted in a reexamination of our laws.

This reexamination resulted in Congress passing a bill, entitled "United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism," six weeks after the attacks on September 11, 2001.[12] It is popularly known as the "USA Patriot Act" (hereinafter the "Patriot Act"). The Patriot Act is a bold but measured piece of legislation that addresses a number of problems with previously existing legal restrictions impairing our ability to respond to the terrorist threat, while preserving fundamental constitutional principles.

Many of our most important intelligence gathering laws were enacted decades ago, in and for an era of rotary telephones. Meanwhile, the terrorists are using e-mail, the Internet, mobile communications and voice mail. Our laws are dependent on jurisdictional boundaries, while terrorists quickly and stealthily move from one jurisdiction to the next. Title II of the Patriot Act[13] modernizes and addresses the gaps in the coverage of the federal electronic surveillance statutes (specifically the wiretap statute, the pen registers and trap and trace statute, and the Electronic Communications Privacy Act (ECPA)). The key feature common among these amendments is the goal of making the statutes technology-neutral. That is, these new provisions ensure that the same existing authorities that apply to telephones are also applicable to computers and use of e-mail on the Internet. It is important to note, however, that the scope of law enforcement authority remains the same; in other words, that no more or less information that is obtainable on one device may be gleaned from another. As illustrated below, by adjusting existing authorities, the new law lives up to its title by "Providing Appropriate Tools Required to Intercept and Obstruct Terrorism."

Section 209 of the Patriot Act amended the law so that law enforcement can now obtain unopened voice-mail stored on a computer server (such as the voice-mail service provided by a local telephone company) with a standard federal search warrant,[14] instead of a wiretap order.[15] It also conclusively established that a wiretap order was not required to retrieve messages from a standard answering machine. Under previous law, the ECPA[16] governed law enforcement access to stored electronic communications (e-mail) but not stored wire communications (voice-mail). Instead, access to stored voice-mail was governed by the wiretap statute, because the definition of "wire communication" included stored communications.[17] Therefore, law enforcement authorities were required to use a wiretap order to obtain voice communications stored with a third party provider, while in some jurisdictions they could use a search warrant if that same information was stored on an answering machine inside a suspect's home. Since both wiretap and search warrant affidavits require a showing of probable cause and stored voice communications possess few of the sensitivities associated with the real-time interception of telephones, the extremely burdensome and time-consuming process of obtaining a wiretap order was unreasonable.

The statutory framework for communication interceptions conceptualized a world in which voice communications via telephones were distinct from non-voice communications (e-mail, faxes, pager messages). The framework did not anticipate, and therefore did not reflect, the convergence of these two kinds of communications common in modern telecommunications networks. With current technology, an e-mail may include one or more attachments consisting of any type of data, including voice recordings. As a result, a law enforcement officer would be in a quandary when, while seeking to obtain a suspect's unopened e-mail from an ISP with a search warrant pursuant to the ECPA, he would find voice attachments (wire communications) which required him to have a wiretap order to open. The Patriot Act, Section 209, provided a practical solution without diminution of the protection of privacy rights.

In Section 211 of the Patriot Act, Congress harmonized current technology with two different sets of legal rules written decades ago. The "Cable Act,"[18] passed in 1984 when cable companies provided only traditional cable programming services, encompasses a very restrictive system of rules governing law enforcement access to most records possessed by a cable company. Accordingly, law enforcement could not obtain records with a subpoena or even a search warrant. Instead, investigators had to demonstrate "clear and convincing evidence" (more than probable cause) that the subscriber was "reasonably suspected" of engaging in criminal activity. But first, the cable company had to provide prior notice to the customer that his records were being sought, an obvious problem for law enforcement. Now that cable companies provide Internet access and telephone service, along with cable programming services, the Cable Act presented a safe haven from law enforcement scrutiny for terrorists' Internet and telephone activity.

Section 211 solved the problem by amending the Cable Act[19] to clarify that the ECPA, the wiretap statute, and the trap and trace statute govern disclosures by cable companies that relate to the providers of communication services, such as telephones and Internet. At the same time, the amendment preserves the Cable Act's higher standard of protection for records regarding ordinary cable television programming.

Terrorists and other criminals often use aliases in registering for Internet and telephone services. This creates an obvious problem for law enforcement attempting to identify the suspects of terrorist acts or criminal acts that often support the terrorists. While the government currently can subpoena electronic communications or a remote computing services provider for the suspect's name, address and length of service, this information does not help when the suspected terrorist lies about his or her identity. Section 210 of the

Patriot Act expanded the type of information law enforcement may obtain with an administrative subpoena to the means and source of payment, including any credit card or bank account number. Permitting investigators to obtain credit card and other payment information significantly assists investigators in tracking a suspect and establishing his/her true identity.

In the overhaul of the technology-related statutes, Section 216 of the Patriot Act amended the law of pen registers and trap and trace devices.[20] When enacted in 1986, the pen/trap statute contemplated only telephone communications, as reflected in its telephone-specific definitions. For example, the statute defined "pen register" as "a device which records or decodes electronic or other impulses which identify the *numbers* dialed or otherwise transmitted on the *telephone line* to which such device is *attached.*"[21] With the advent of the electronic communications explosion, investigators needed comparable access to non-content information being communicated with e-technology. Section 216 amended the pen/trap provisions to clarify that the statute applies to electronic communications, as well as wire. Accordingly, with these amended definitions, law enforcement can intercept e-mail header information upon certification to the court that the information is likely to be obtained by an installed pen register or trap and trace device and its use is relevant to an ongoing criminal investigation.

Prior to the Patriot Act, the pen/trap statute allowed the court to authorize pen register/trap and trace installations only "within the jurisdiction of the court."[22] In other words, if a telephone was located, for example, in the District of New Jersey, but the substantive investigation was in the District of Delaware, then the Delaware Assistant U.S. Attorney was required to obtain the pen register/trap and trace orders from a New Jersey District judge. With the deregulation in the telecommunications industry, a single communication may be carried by many providers — from a local exchange carrier, to a local Bell operation, to a long distance carrier, to a local exchange carrier in another jurisdiction, to a cellular carrier — all located in different jurisdictions. This process imposed time delays and burdens on both the U.S. Attorney Offices and the Federal courts. Congress recognized the negative consequences of the situation when it drafted Section 216: "Currently, the government must apply for a new pen/trap order in every jurisdiction where the target telephone is located. This can cause serious delays that could be devastating to an investigation, particularly where additional criminal or terrorist acts are planned.... This section authorizes the court with jurisdiction over the offense of the investigation to issue the order, thus streamlining an investigation and eliminating the need to intrude upon the resources of courts and prosecutors with no connection to the investigation."[23]

Congress streamlined the process for multi-jurisdictional investigations by amending the statute in two ways. First, it gave authority to the federal courts to compel assistance from any communication service provider in the United States whose assistance "may facilitate the execution of the order."[24] The court may do so upon the government's certification that the information "likely to be obtained . . . is relevant to an ongoing criminal investigation . . ."[25] Second, the amended statute eliminated the requirement that a federal pen/trap order specify its geographic limit, thereby giving nationwide effect for such orders upon a showing that the issuing court has jurisdiction over the particular crime under investigation.[26] This double dose of practicality facilitates law enforcement in catching up with suspected terrorists, who know no jurisdictional boundaries, in time to foil plans intended to harm our citizens.

This multi-jurisdictional approach was repeated by Congress in amending Fed.R.Crim.Proc. 41(a) by Section 219 of the Patriot Act. Now, a federal magistrate judge, in a district in which domestic or international terrorism activities are occurring, may authorize a search for property or a person in any location in the country. For all other crimes, the law remains the same in that the judge may authorize a search only within the judge's district. Likewise, in Section 220, the Patriot Act amended section 2703(a) of title 18, United States Code, to authorize courts with jurisdiction over the criminal offenses to issue search warrants for electronic communications stored anywhere in the United States, rather than in the district where the "property" was located.

Even though jurisdictional lines fall and legal hurdles lower with these amendments, privacy rights are still protected by the same constitutional standards. Making it easier for government entities to detect and fight terrorism does not mean that U.S. citizens fall victim to tyranny. Title II of the Patriot Act, as highlighted above, modified and clarified the law of communication interceptions conducted by law enforcement, while maintaining the Fourth Amendment protection to the right to privacy. To counterbalance this intrusive law enforcement power, in Section 223 of the Patriot Act Congress strengthened the Inspector General oversight into, and civil liability for, the suspected willful or intentional interception or disclosure of information derived from an interception.

The success of our war against terrorism will be measured, in part, by the number of terrorist acts detected and prevented or averted. To protect sources and methods, U.S. law enforcement and intelligence agencies will not be at liberty to publicize most of their successful efforts. Therefore, the American public will likely never know the whole value of our anti-terrorism forces and the role played by the USA Patriot Act. ❖

Footnotes:
References available upon request. Contact editorial@mediatwo.com.

Drew Fennell

THE USA PATRIOT ACT: CAN WE BE BOTH SAFE AND FREE?

> The Constitution of the United States is a law for rulers and people, equally in war and in peace, and covers within the shield of its protection all classes of men, at all times, and under all circumstances. No doctrine, involving more pernicious consequences, was ever invented by the wit of man than that any of its provisions can be suspended during any of the great exigencies of government. Such a doctrine leads directly to anarchy or despotism, but the theory of necessity on which it is based is false; for the government, within the Constitution, has all the powers granted to it, which are necessary to preserve its existence.
>
> Ex Parte Milligan, 71 U.S. 2, 120-21 (1866)

On October 25, 2001, a matter of weeks after September 11, the U.S. Congress passed the USA Patriot Act, a bill that contains the most sweeping and comprehensive changes in domestic law enforcement in history, with very little discussion and almost no dissent. Members of Congress had little opportunity to review the bill before its passage. The Act is hundreds of pages long and amends scores of sections of the U.S. Code. However, many members of Congress, barred from their offices during the anthrax scare, were unable to read the entire bill, much less undertake a close analysis of its provisions.

Even now, a year and a half after its passage, the USA Patriot Act has not been codified. That is, there is no version that shows all of the changes to existing law made by the Act. Anyone who wants to view the Act as a whole must look at the Public Law as passed by Congress, which does not place any of the changes in their context in the U.S. Code.[1] Because the USA Patriot Act changed the wording of many different statutes within the U.S. Code, this lack of a codified version makes it difficult to examine the changes in a comprehensive way.[2]

The acronym USA Patriot stands for Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. As the title suggests, most of its provisions apply to surveillance and law enforcement. Many provisions of the Patriot Act were necessary changes to statutes that were no longer relevant to emerging technology or that did not take into account the changing world stage in which individuals, unaffiliated with any government, might pose a threat to national security. Other provisions pose grave threats to the freedoms guaranteed under the Constitution. At its extremes, the USA Patriot Act gives the government expanded power to invade privacy, imprison people without due process, and punish dissent.

This article examines only those provisions that have the deepest impact on our Constitutional rights. Of necessity, it does not address large portions of the USA Patriot Act, including some provisions that pose troubling questions about the relationship of liberty and law enforcement. For example, this article does not address certain complex issues such as enhanced border protections, financial disclosure provisions and other amendments to the Bank Secrecy Act, changes to the currency and money laundering statutes, or criminal statutes.

Domestic Terrorism Defined

Section 802 of the USA Patriot Act expands the definition of terrorism to include "domestic" as opposed to international terrorism. A person engages in domestic terrorism if he does an act "dangerous to human life" that is a violation of the laws of a state or the United States, if the act appears to be intended to: (i) intimidate or coerce a civilian population; (ii) influence the policy of a government by intimidation or coercion; or (iii) affect the conduct of a government by mass destruction, assassination, or kidnapping.[3] Additionally, the acts have to occur primarily within the territorial jurisdiction of the United States, and if they do not, may be regarded as international terrorism.

Section 802 does not create a new crime of domestic terrorism. Instead, it expands the type of conduct that the government may investigate as "terrorism." This definition of terrorism is broad enough to encompass the activities of several prominent activist groups such as Greenpeace, Operation Rescue, and the Vieques Island protesters, a group that included Robert F. Kennedy, Jr., U.S. Representative Luis Guitierrez, D-Ill., and Jacqueline Jackson, wife of Rev. Jesse Jackson. Any person engaging in civil disobedience that has the potential for danger to human life, including their own, can be investigated for terrorism under Section 802. For example, the tree-sitters who live high in the trees of the California redwood forest, meet the definition of domestic terrorist.

Civil Forfeiture

Section 806 authorizes the civil forfeiture of all assets, foreign or domestic (i) of any individual, entity, or organization engaged in planning or perpetrating acts of domestic or for-

eign terrorism against the United States, or their property, and all assets, foreign and domestic, affording any person a source of influence over any such entity or organization or (ii) acquired or maintained by any person with the intent and for the purpose of supporting, planning, conducting, or concealing an act of domestic or international terrorism against the United States, citizens or residents of the United States or their property (iii) derived from, involved in, or used or intended to be used to commit any act of domestic or international terrorism against the United States, citizens or residents of the United States or their property.

Section 806 could result in the civil seizure of assets of an individual or organization without a hearing and without a criminal conviction. Not only would individuals actually involved in protests that meet the definition of domestic terrorism be subject to forfeiture of their assets, so would any individuals or organizations supporting the protests.

Sections 802 and 806 have already been used to chill public protest unrelated to foreign terrorism. Recently, a large paper manufacturer notified a charitable foundation that had given monetary support to environmental activists that the paper company had asked the Department of Justice to investigate the foundation for material support of domestic terrorism. The USA Patriot Act provides a powerful tool against logging protests.

The civil asset forfeiture power of the U.S. government is awesome. The government can seize or freeze assets on a bare assertion that there is probable cause that the assets were involved in domestic terrorism. The assets are seized without a hearing and often without notice. In order to permanently forfeit the assets, the government must go before a court, but in a civil proceeding where the standard is the preponderance of the evidence and where the person is not entitled to be represented at public expense as they would be in a criminal proceeding. Defending against forfeiture could easily bankrupt an organization if the government asserts that it is involved in domestic terrorism.

Foreign Intelligence Surveillance Act Wiretap and Black Bag Searches

The Foreign Intelligence Surveillance Act (FISA)[4] was enacted in the wake of Watergate to provide a bulwark between foreign intelligence gathering and domestic criminal investigations following the FBI's abuse of its investigatory powers against Dr. Martin Luther King and others. FISA was created in part to allow foreign intelligence investigations to proceed without having to comply with Fourth Amendment requirements. Put simply, because FISA surveillance warrants were not to be used in criminal investigations, the Fourth Amendment did not apply. Section 218 of the USA Patriot Act removes the boundary between foreign intelligence gathering and criminal investigation. Previously, FISA required that the FBI could only execute a wiretap or physical ("black bag") search that did not comply with the Fourth Amendment if "the purpose" was to gather foreign intelligence. Section 218 replaces "the purpose" with "significant purpose," allowing the FBI to evade the Fourth Amendment even when its principal goal is criminal law enforcement.

On May 17, 2003 the Foreign Intelligence Surveillance Court released an unprecedented public opinion in which it rejected Attorney General Ashcroft's proposal to replace FISA procedures with new rules that would allow information to be shared with law enforcement officials and argued specifically that the USA Patriot Act "allow[s] FISA to be used primarily for a law enforcement purpose." In a unanimous decision, the FISC ruled that law enforcement officials "shall not make recommendations to intelligence officials concerning the initiation, operation, continuation or expansion of FISA searches or surveillances."

The Department of Justice filed an appeal and the FISA Court of Review met for the first time in its twenty-four-year history. There had never been an appeal before, primarily because FISA hearings are ex parte and the government is the only party to be heard. Therefore, the government is the only party that can appeal. The FISA Court of Review reversed the lower court and ruled in favor of the Justice Department's argument that the USA Patriot Act allows FISA warrants to be issued even if foreign intelligence is not the primary purpose of the surveillance. It is unclear whether there can be any further appeal, because the Justice Department is the only party to the ruling and no other interested parties were able to establish standing in the FISA Court of Appeal.

Access to Records

Section 215 of the USA Patriot Act amends FISA and allows the FBI to require anyone at all (including libraries, bookstores, and internet service providers) to give its records or other "tangible things" to the government. There is no requirement, as there would be under the Fourth Amendment, for the FBI to show probable cause or even reasonable suspicion of criminal activity. All the FBI must do is to assert that the request for records is related to an ongoing terrorism investigation. There is essentially no judicial oversight, because the FISA court is required to issue the order if the application meets certain minimal formal requirements.[5]

Section 215 orders can be served on U.S. citizens and may be based in part on a person's First Amendment activities. No notice is provided to the person whose records are sought. Indeed, the party from whom the FBI obtained records is prohibited under penalty of law from disclosing to anyone, including the subject of the request, that the FBI made the request.[6]

These surreptitious searches of third party records raise a number of issues under the Fourth and Fifth Amendments and the gag provisions raise First Amendment concerns for the third parties who have provided the records. Librarians, university registrars, bookstore owners and others who have been frequent targets of these requests have been organizing to publicize the existence of Section 215 and to explore litigation strategies. Litigation is particularly difficult because the statutory scheme does not provide for a challenge such as a motion to quash a subpoena issued under the Fourth Amendment. Further, the target of the search cannot challenge the search unless the party providing the records violates the gag provisions of Section 215. In assessing the potential harm of this section, note that *any* entity or person can be required to disclose records. For example, the ACLU or other advocacy organization could be forced to share its membership lists.

Electronic Surveillance

A large portion of the USA Patriot Act changes the rules of electronic surveillance by amending the Electronic Communications Privacy Act (ECPA) and the Foreign Intelligence Surveillance Act (FISA).[7] For example, Section 209 amends ECPA to allow the seizure of voice-mail messages on the same basis as stored electronic messages. Therefore, federal officers do not need

to meet the more stringent requirements that apply to interception of live telephone conversations.[8] Under Section 210, the government can require communication service providers to disclose "means and source of payment for such services (including credit card or bank account numbers)."

Section 216 changes the regulation of pen registers and tap and trace devices. Pen registers have traditionally been used to provide lists of phone numbers to investigators without providing any content. Interceptions that captured content were subject to the more stringent requirements of the wiretapping statutes. Prior to the USA Patriot Act, the government was required to restrict recording and decoding to "dialing and signaling information used in call processing" so that content information was fully protected. Under Section 216, the government will now be able to use a pen register or tap and trace device to obtain website addresses and e-mail addresses, although such addresses contain content. In fact, e-mail messages move together in packets that contain both address and content information. Section 216 also appears to authorize the use of Carnivore, a system that intercepts and examines all forms of internet activity. Once installed, Carnivore will intercept not only the communications of targeted individuals, but all e-mail messages, web page activity, and telephone conversations that flow through the internet. Although the FBI promises that it will use filters to weed out information it is not authorized to see, this system is ripe for abuse and there is no provision for judicial or legislative oversight.

Single Jurisdiction Search Warrants

Section 219 amends Rule 41(a) of the Federal Rules of Civil Procedure to authorize the government to go before a single magistrate in any district in which activities related to terrorism may have occurred and to obtain a warrant to search persons or property within or outside the district.[9] This means that meaningful judicial oversight will be very difficult. A person in California who seeks to quash a warrant issued in New York will have to travel to New York in order to appear before the court that issued the warrant, a daunting task for most.

Sneak and Peak Searches and Delayed Notice of Execution of a Warrant

Section 213 permits delayed notification of the execution of so-called "sneak and peek" warrants, which would otherwise be impermissible under Rule 41(d) of the Federal Rules of Criminal Procedure. A "sneak and peek" warrant is one that authorizes the government to secretly enter (either electronically or physically) to conduct a search, observe, take measurements, conduct examinations, take photos, copy documents, download or transmit computer files and depart without taking any tangible evidence. In the absence of Section 213, those executing the warrant must leave a copy of the warrant and an inventory of what they seized. Under 213, this notice may be delayed until long after the search is completed. This lack of notice prevents the subject of the search from bringing any objection before the court in a timely manner and may infringe on the Fourth Amendment rights to be free from unreasonable or warrantless searches.

Immigration Laws

The USA Patriot Act makes a number of changes to immigration law. Section 411 defines factors that make an alien ineligible for admission to United States. No one may be admitted who has engaged in terrorist activity, including soliciting on behalf of a terrorist organization or providing material support to a terrorist organization. An individual who uses his or her place of prominence to endorse, espouse, or advocate for terrorist activities or organizations is not admissible. The spouse or child of any inadmissible person is likewise inadmissible. But what is a terrorist organization? For purposes of this section, a terrorist organization is not only an organization that engages in terrorism, but also any organization that provides material support to a terrorist organization. Here we see the same second and third order effects that we saw above under the domestic terrorism definitions. Someone who gave money to an organization that gave money to an organization that provided material support for terrorism may be declared inadmissible.

Under Section 412 of the USA Patriot Act, the Attorney General may detain alien suspects for up to seven days without initiating deportation or criminal proceedings merely by certifying that the detainee is suspected of terrorism, espionage, or sedition, or is otherwise deportable or inadmissible. Once those proceedings are initiated, the Attorney General must review the certification every six months. The Attorney General's certification is subject to review only under a writ of habeas corpus to the federal courts and can be appealed only to the U.S. Court of Appeals for the District of Columbia.[10] What this means in practice is that anyone who is even suspected of falling into the rather loose categories outlined above may be detained, certainly for seven days, and perhaps indefinitely. Since September 11, large numbers of individuals have been detained, many of them under this provision. The Justice Department has steadfastly refused to provide any information regarding these detentions, declining even to disclose the number of detainees. Instead, they have closed all immigration hearings to the public.

Non-citizens report that they are fearful of any encounter with law enforcement and are reluctant to report crimes, even when they are the victims. Some have reported that they will not engage in anything as simple as fighting a traffic ticket for fear that they might be accused of something worse. Many members of immigrant communities keep a low profile and are so reluctant to engage with law enforcement officials that they are unlikely to provide needed information about activities the government should investigate.

Patriot II

Recently, new draft legislation has surfaced. This new legislation has not been introduced to Congress, but has been circulating on Capitol Hill. Among its more controversial provisions it would make it easier to obtain FISA warrants, which will be available for investigation of "unaffiliated individuals" even if they are not tied to any terrorist organization. It would permit the government to bypass the FISA court in some instances and conduct warrantless wiretaps and searches. It would create a new category of "domestic security surveillance" that would permit electronic eavesdropping under looser standards than those that apply to criminal investigations. It would give the government secret access to credit reports. It would allow the government to access records available under Section 215 of the USA Patriot Act even for investigation of domestic crimes. It would allow the government to strip the citizenship of any American who provides support to a group designated by the Justice Department as a terrorist organization. It would cancel state and federal court

orders that prevent local law enforcement agencies from spying on community activists. It would create a DNA database of "suspected terrorists" which would provide for the voluntary taking of DNA samples from persons who have neither been charged or convicted of any crime. Failure to comply with "voluntary" sampling would be a crime.

Public criticism of the USA Patriot Act has come from all corners of the political spectrum, including well-known political conservatives such as former Congressman Dick Armey, Grover Norquist of Americans for Tax Reform, Ken Connor of the Family Research Council, and Paul Weyrich of the Free Congress Foundation. Criticism of Patriot II by a wide variety of voices has also been loud and swift, causing the Justice Department to distance itself from the draft legislation, claiming that no one in a position of authority had any input. Perhaps public opinion will be strong enough to prevent Patriot II from being introduced in Congress.

Conclusion

The USA Patriot Act rolls back many of the protections that were enacted into law in response to government abuses of power — the Palmer Raids of the 1920s in which thousands of Italian immigrants were illegally detained, the mass internments of Japanese Americans during World War II, the excesses of McCarthyism, and the abuses of domestic intelligence against civil rights activists and war protesters in the 1960s. Ultimately, it would be wise to remember that history teaches that government can be a powerful threat to liberty, personal security, and even life itself. By giving the government vast new powers under the USA Patriot Act, we are not simply "making ourselves safer." We are paradoxically making ourselves less safe. We continue to require protection from a government that can take our liberty, property, livelihoods and lives arbitrarily if Constitutional norms are not respected. We can be both safe and free under the Constitution. Without it we are neither safe nor free. ◆

Footnotes:

References available upon request. Contact editorial@mediatwo.com.

Erin Daly

LET THE SUN SHINE IN: THE FIRST AMENDMENT AND THE WAR ON TERRORISM

In our system of government, the people hold the sovereign power. It is the people who decide who their leaders will be, and it is the people to whom the leaders are accountable. But how can we exercise the rights and responsibilities of citizenship without ample information about the workings of government? As Madison once wrote about the importance of public schools, "A popular Government, without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or, perhaps both. Knowledge will forever govern ignorance: And a people who mean to be their own Governors, must arm themselves with the power which knowledge gives."

Throughout the Supreme Court's First Amendment jurisprudence, it has recognized the importance of this fundamental principle: the central meaning of the First Amendment is that the people must have access to information about public officials and official policies and that government suppression of information not only violates the First Amendment, but interferes with the basic premise of popular sovereignty. "An informed public is the most potent of all restraints upon misgovernment[.]" *Grosjean v. Am. Press Co.* (1936).

Thus, it is often said that sunshine is the best disinfectant — that a government that operates openly operates cleanly. Open meetings laws, public disclosure laws, and freedom of information laws all operate on this premise. *See e.g.* 5 USC §552b "Open Meetings" (Added Sept. 13, 1976, P.L. 94-409, 90 Stat. 1241); 5 USC §552 "Freedom of Information Act (FOIA) (Amended Nov. 21, 1974, P.L. 93-502, 88 Stat. 1561, 5 USCS § 552); Federal Election Campaign Act (2 USC §§ 431 et seq. (Amended 1976)).

Many of the policies of the current administration are in tension with the tradition of exposing government actions to light. In the last few years, we have seen changes in the law and administrative policies that, in the aggregate, indicate an inclination toward secrecy has become a leitmotif of the administration. Some of these new initiatives are necessitated by genuine concern about national security in the wake of September 11; others are not even facially related to the threat of terrorism, but seem justified simply by a preference for secrecy over openness.

An Enlightened Citizenry

Because freedom of speech is integral to a free democracy, the Supreme Court has consistently recognized that political speech is at the "core" of the First Amendment. To that end, it has protected all manner of otherwise unappealing speech — from defamation to lewd cartoons to flag burning — in order to ensure that the public has full access to a range of information and commentary about the government. Two celebrated cases may suffice to make the point.

In *New York Times v. Sullivan* (1964), the Court considered the Montgomery Alabama police commissioner's defamation claim against the *New York Times* "against the background of a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open, and that it may well include vehement, caustic, and sometimes unpleasantly sharp attacks on government and public officials." It ruled, therefore, that before a government official could recover damages for defamation about his official conduct, he needed to prove not only that the publication was false and defamatory but that the defendant had acted with knowledge of the statement's falsity or with reckless disregard of its truth or falsity. The purpose of erecting this almost impossibly high barrier to recovery was precisely to shield newspapers from the specter of crippling defamation suits — to give the First Amendment the "breathing space" it needs to survive. Had Sullivan won his half-million-dollar damage award, newspapers would be significantly more cautious in disseminating even truthful information about government officials; the people would have significantly less information on which to base the exercise of their citizenship rights and duties.

The Court hewed the same line in a case involving the publication of the "Pentagon Papers." In that case, the *New York Times* had obtained just under half of the 47-volume study of the Viet Nam War, researched and written by Pentagon officials themselves. Upon seeing the first two installments of the report featured on the front page of the Times, then Attorney General John Mitchell telegrammed the *Times* (and the *Washington Post* which was also embarking on its own publication of some of the Pentagon papers), and insisted that the newspapers desist from any further publication of the report. An ornery press refused and the government forced the issue in court against both newspapers. With three justices dissenting, a majority of the Supreme Court held only two weeks later that the government had failed to overcome the heavy presumption against prior restraints. *New York Times v. United States* (1971).

The case is remarkable and continues to be relevant because it so clearly raises the question that the government is wrestling with today: how much secrecy can the First Amendment tolerate when national security seems to be at stake? In the *New York Times* case, the government tried to stop the publication of information *about an ongoing war.*

ple, as Madison said, must be armed with information about the government, and the press is the most effective conduit for that information.

In the absence of the governmental checks and balances present in other areas of our national life, the only effective restraint upon executive policy and power in the areas of national defense and international affairs may lie in an enlightened citizenry — in an informed and critical public opinion which alone

Another aspect of secrecy is the refusal to disclose information that by law should be disclosed. On October 12, 2001, Attorney General Ashcroft issued a Memorandum that warned that a decision to disclose information protected under the Freedom of Information Act should only be made after "full and deliberate consideration" of the countervailing interests that could be implicated by disclosure. The Memorandum went on to assure agency officials that decisions to *withhold* information under the Freedom of Information Act would be defended in court "unless they lack a sound legal basis or present an unwarranted risk of adverse impact on the ability of other agencies to protect other important records." (Available at http://www.fas.org/sgp/foia/ashcroft.html). The Memorandum's reach is not limited to those records that have a demonstrated relation to national security but applies broadly to all FOIA requests. This departs from the practice and letter of FOIA which requires disclosure of covered records, regardless of need, unless there is a particular reason why disclosure would be harmful for specified reasons.

In March 2003, President Bush signed an Executive Order that, according to Steven Aftergood of the Secrecy Project of the Federation of American Scientists, includes "several changes tending in the direction of greater secrecy," although he notes that the order does not change the basic structure of classification and declassification in effect since the Clinton administration. The changes the Executive Order does make include: 1) eliminating the presumption of declassification or of lower classification level in cases of "significant doubt"; 2) requiring training on "the criminal, civil, and administrative sanctions that may be brought against an individual who fails to protect classified information from unauthorized disclosure"; 3) postponing automatic declassification for an additional three years; and 4) permitting the reclassification of documents that have already been made public, among other things. ("Further Amendment to Executive Order 12958, As Amended, Classified National Security Information," March 25, 2003). While the Order refers by name to "national security," its content extends to all classified materials, regardless of their nexus to national security. For instance, a narrower order might have required a higher level of classification in cases of significant doubt only where the record in question bears directly on national security.

This new policy supplements Executive Order 13,233 ("Further Implementation of the Presidential Records Act," November 1, 2001) which changed the rules governing disclosure of presidential papers. Under federal law, outgoing presidents could protect their papers from disclosure for up to 12 years after they left office;

LET T
THE FI
THE

In our system of government, sovereign power. It is the peopl leaders will be, and it is the peo are accountable. But how can w responsibilities of citizenship wit about the workings of governn wrote about the importance of ular Government, without popu means of acquiring it, is but a P Tragedy; or, perhaps both. govern ignorance: And a people whc Governors, must arm themselves knowledge gives."

Throughout the Supreme Cou jurisprudence, it has recognized the in mental principle: the central meaning is that the people must have access to lic officials and official policies and th sion of information not only violates but interferes with the basic premise "An informed public is the most pote misgovernment[.]" *Grosjean v. Am. P*

Thus, it is often said that sunshine — that a government that operates Open meetings laws, public disclosur information laws all operate on this §552b "Open Meetings" (Added Se 409, 90 Stat. 1241); 5 USC §552 "F Act (FOIA) (Amended Nov. 21, 197 1561, 5 USCS § 552); Federal Elec USC §§ 431 et seq. (Amended 1976

Many of the policies of the curre tension with the tradition of exposing light. In the last few years, we have and administrative policies that, in th inclination toward secrecy has become a leitmotif of the administration. Some of these new initiatives are necessitated by genuine concern about national security in the wake of September 11; others are not even facially related to the threat of terrorism, but seem justified simply by a preference for secrecy over openness.

An Enlightened Citizenry

Because freedom of speech is integral to a free democracy, the Supreme Court has consistently recognized that political speech is at the "core" of the First Amendment. To that end, it has protected all manner of otherwise unappealing speech — from defamation to lewd cartoons to flag burning — in tion of the report. An ornery press refused and the government forced the issue in court against both newspapers. With three justices dissenting, a majority of the Supreme Court held only two weeks later that the government had failed to overcome the heavy presumption against prior restraints. *New York Times v. United States* (1971).

The case is remarkable and continues to be relevant because it so clearly raises the question that the government is wrestling with today: how much secrecy can the First Amendment tolerate when national security seems to be at stake? In the *New York Times* case, the government tried to stop the publication of information *about an ongoing war.*

ple, as Madison said, must be armed with information about the government, and the press is the most effective conduit for that information.

In the absence of the governmental checks and balances present in other areas of our national life, the only effective restraint upon executive policy and power in the areas of national defense and international affairs may lie in an enlightened citizenry — in an informed and critical public opinion which alone

Another aspect of secrecy is the refusal to disclose information that by law should be disclosed. On October 12, 2001, Attorney General Ashcroft issued a Memorandum that warned that a decision to disclose information protected under the Freedom of Information Act should only be made after "full and deliberate consideration" of the countervailing interests that could be implicated by disclosure. The Memorandum went on to assure agency officials that decisions to *withhold* information under the Freedom of Information Act would be defended in court "unless they lack a sound legal basis or present an unwarranted risk of adverse impact on the ability of other agencies to protect other important records." (Available at http://www.fas.org/sgp/foia/ashcroft.html). The Memorandum's reach is not limited to those records that have a demonstrated relation to national security but applies broadly to all FOIA requests. This departs from the practice and letter of FOIA which requires disclosure of covered records, regardless of need, unless there is a particular reason why disclosure would be harmful for specified reasons.

In March 2003, President Bush signed an Executive Order that, according to Steven Aftergood of the Secrecy Project of the Federation of American Scientists, includes "several changes tending in the direction of greater secrecy," although he notes that the order does not change the basic structure of classification and declassification in effect since the Clinton administration. The changes the Executive Order does make include: 1) eliminating the presumption of declassification or of lower classification level in cases of "significant doubt"; 2) requiring training on "the criminal, civil, and administrative sanctions that may be brought against an individual who fails to protect classified information from unauthorized disclosure"; 3) postponing automatic declassification for an additional three years; and 4) permitting the reclassification of documents that have already been made public, among other things. ("Further Amendment to Executive Order 12958, As Amended, Classified National Security Information," March 25, 2003). While the Order refers by name to "national security," its content extends to all classified materials, regardless of their nexus to national security. For instance, a narrower order might have required a higher level of classification in cases of significant doubt only where the record in question bears directly on national security.

This new policy supplements Executive Order 13,233 ("Further Implementation of the Presidential Records Act," November 1, 2001) which changed the rules governing disclosure of presidential papers. Under federal law, outgoing presidents could protect their papers from disclosure for up to 12 years after they left office;

LET T
THE FI
THE

In our system of government, sovereign power. It is the peopl leaders will be, and it is the peo are accountable. But how can w responsibilities of citizenship wit about the workings of governm wrote about the importance of ular Government, without popu means of acquiring it, is but a P Tragedy; or, perhaps both. govern ignorance: And a people who Governors, must arm themselves v knowledge gives."

Throughout the Supreme Cou jurisprudence, it has recognized the in mental principle: the central meaning is that the people must have access to lic officials and official policies and th sion of information not only violates but interferes with the basic premise "An informed public is the most pote misgovernment[.]" *Grosjean v. Am. P*

Thus, it is often said that sunshine — that a government that operates Open meetings laws, public disclosur information laws all operate on this §552b "Open Meetings" (Added Se 409, 90 Stat. 1241); 5 USC §552 "F Act (FOIA) (Amended Nov. 21, 197 1561, 5 USCS § 552); Federal Elec USC §§ 431 et seq. (Amended 1976)

Many of the policies of the currer tension with the tradition of exposing light. In the last few years, we have s and administrative policies that, in th inclination toward secrecy has become a hallmark of the administration. Some of these new initiatives are necessitated by genuine concern about national security in the wake of September 11; others are not even facially related to the threat of terrorism, but seem justified simply by a preference for secrecy over openness.

An Enlightened Citizenry

Because freedom of speech is integral to a free democracy, the Supreme Court has consistently recognized that political speech is at the "core" of the First Amendment. To that end, it has protected all manner of otherwise unappealing speech — from defamation to lewd cartoons to flag burning — in tion of the report. An ornery press refused and the government forced the issue in court against both newspapers. With three justices dissenting, a majority of the Supreme Court held only two weeks later that the government had failed to overcome the heavy presumption against prior restraints. *New York Times v. United States* (1971).

The case is remarkable and continues to be relevant because it so clearly raises the question that the government is wrestling with today: how much secrecy can the First Amendment tolerate when national security seems to be at stake? In the *New York Times* case, the government tried to stop the publication of information *about an ongoing war.*

The national security argument could not have been stronger. And still, the justices insisted on a strong evidentiary showing that publication of specific materials would cause serious harm. "[O]nly governmental allegation and proof that publication must inevitably, directly, and immediately cause the occurrence of an event kindred to imperiling the safety of a transport already at sea can support even the issuance of an interim restraining order. In no event may mere conclusions be sufficient: for if the Executive Branch seeks judicial aid in preventing publication, it must inevitably submit the basis upon which that aid is sought to scrutiny by the judiciary."

Indeed the fact that the information related to an ongoing war may have made the government's case harder, not easier: how could the government shield from view vital information about a public policy of such magnitude? As Justice Black said, "[P]aramount among the responsibilities of a free press is the duty to prevent any part of the government from deceiving the people and sending them off to distant lands to die of foreign fevers and foreign shot and shell."

Part of the reason for a specific showing of harm is to ensure that no more speech than necessary is suppressed. Another reason is to prevent the government from hiding behind a curtain of national security when its real concern is less noble. As Justice Douglas said, "[t]he dominant purpose of the First Amendment was to prohibit the widespread practice of governmental suppression of embarrassing information." The First Amendment does not allow the suppression of vast amounts of information on the undocumented claim that disclosure *could* harm national security.

Both of these cases, along with scores of others, recognize that free speech is essential to democracy and that a free press is essential to free speech. In order to exercise their sovereign rights, people, as Madison said, must be armed with information about the government, and the press is the most effective conduit for that information.

In the absence of the governmental checks and balances present in other areas of our national life, the only effective restraint upon executive policy and power in the areas of national defense and international affairs may lie in an enlightened citizenry — in an informed and critical public opinion which alone can here protect the values of democratic government. For this reason, it is perhaps here that a press that is alert, aware, and free most vitally serves the basic purpose of the First Amendment. For without an informed and free press there cannot be an enlightened people. (*New York Times v. U.S.* (Stewart J. conc.))

In the Dark

Many of the current administration's policies have proceeded on the opposite presumption: that information is likely to be dangerous if released and that the burden is on those who seek information to prove their bona fides. Some of this heightened concern about disclosure may be justified by a post-September 11 heightened awareness of the risks involved in divulging too much information. But many of the Bush administration initiatives and practices are facially unrelated to national security or sweep so broadly that they shield from view substantial amounts of useful and presumptively harmless information about the operations of government. The overall picture is of an administration that is unduly inclined towards secrecy, at the expense of public debate and to the detriment of the citizenry.

Sharing information with the public

In a variety of ways, the Bush Administration has shown a disinclination to share information, formally or informally, with the public. Examples of this might include the reduced number of press conferences that the President has given since he has been in office. Even since the onset of the war on terrorism, he has given only two: one about one month after September 11, 2001, and one on the eve of war in Iraq in March 2003. All other questions by the press to the President are fielded by other administration officials and information from the President is now managed by the White House's own Office of Global Communications. This shuts off discussion not only about matters relating to national security, but about all other matters of public concern as well.

Another aspect of secrecy is the refusal to disclose information that by law should be disclosed. On October 12, 2001, Attorney General Ashcroft issued a Memorandum that warned that a decision to disclose information protected under the Freedom of Information Act should only be made after "full and deliberate consideration" of the countervailing interests that could be implicated by disclosure. The Memorandum went on to assure agency officials that decisions to *withhold* information under the Freedom of Information Act would be defended in court "unless they lack a sound legal basis or present an unwarranted risk of adverse impact on the ability of other agencies to protect other important records." (Available at http://www.fas.org/sgp/foia/ashcroft.html). The Memorandum's reach is not limited to those records that have a demonstrated relation to national security but applies broadly to all FOIA requests. This departs from the practice and letter of FOIA which requires disclosure of covered records, regardless of need, unless there is a particular reason why disclosure would be harmful for specified reasons.

In March 2003, President Bush signed an Executive Order that, according to Steven Aftergood of the Secrecy Project of the Federation of American Scientists, includes "several changes tending in the direction of greater secrecy," although he notes that the order does not change the basic structure of classification and declassification in effect since the Clinton administration. The changes the Executive Order does make include: 1) eliminating the presumption of declassification or of lower classification level in cases of "significant doubt"; 2) requiring training on "the criminal, civil, and administrative sanctions that may be brought against an individual who fails to protect classified information from unauthorized disclosure"; 3) postponing automatic declassification for an additional three years; and 4) permitting the reclassification of documents that have already been made public, among other things. ("Further Amendment to Executive Order 12958, as Amended, Classified National Security Information," March 25, 2003). While the Order refers by name to "national security," its content extends to all classified materials, regardless of their nexus to national security. For instance, a narrower order might have required a higher level of classification in cases of significant doubt only where the record in question bears directly on national security.

This new policy supplements Executive Order 13,233 ("Further Implementation of the Presidential Records Act," November 1, 2001) which changed the rules governing disclosure of presidential papers. Under federal law, outgoing presidents could protect their papers from disclosure for up to 12 years after they left office;

thereafter presidential papers would be available to the public under the same terms as all other records under FOIA. At the point when President Reagan's papers would have become available under FOIA, President Bush issued an executive order changing the procedures. Under the new rules, upon the expiration of the 12 years, any request for access to presidential documents must be acceded to both by the former president and by the incumbent president. In addition, requests for access must be justified by a "demonstrated, specific need" for the particular records, in contrast to the FOIA under which no showing of need is required at all.

Sixty-eight thousand papers, including those relating to the Iran-Contra affair, which implicates many current administration officials, are now presumptively *un*available, rather than being statutorily available. This will not only affect the right of access of citizens about information generally, but also the right of researchers and historians to learn about and document decisions of government. (Indeed, the American Historical Association is the name plaintiff in a suit challenging the legality of the order). The loss of information is not counterbalanced by any apparent gain in security.

This government has also kept secret substantial information about its criminal law enforcement efforts since September 11, in contravention of historical practice. Secret arrests have never been a practice that this country has countenanced, but since September 11 there have been hundreds of people whose arrests have been shielded from public oversight. The government has refused to disclose the number of people who have been detained since September 11 as material witnesses or in violation of their visas; their names, locations, and the charges against them have all been kept secret. Moreover, deportation hearings that have unilaterally been designated as of "special interest" have been kept secret, along with even the fact, or not, of whether a deportation hearing even took place. Nor have the names of the hundreds of individuals being held by the United States government in Guantanamo Bay been released. While these practices of non-disclosure bear only the Executive's imprimatur so far, the new Domestic Security Enhancement Act would codify the practices by immunizing from disclosure under FOIA additional information relating to arrests and detention.

From the perspective of the defendants' and the public's interest in ensuring that government authorities act within constitutional limits, this secrecy makes it impossible to know if defendants in immigration or criminal proceedings have been given due process of law and otherwise been treated fairly. It makes it impossible to know if the government has made a mistake about a person's identity or a person's involvement in unlawful activity, which can happen from time to time. It makes it impossible to know if the government is targeting certain individuals on the basis of their race or creed or associational activities, which has also been known to happen, especially in times of war. On the other hand, it also makes it impossible to know if the government's policies have been effective in protecting Americans from threats of terrorism. No one arrested under this policy has, as far as we know, been charged with terrorism-related crimes.

Sharing information with Congress

Many members of Congress — including individuals in Mr. Bush's own wing of his party, have criticized the Administration for failing to share important information with them. The executive's recalcitrance impedes Congress's ability to exercise its constitutional and statutory obligations relating to oversight and budget management, among other things. In June 2002, several members of Congress, including conservative members such as former Congressman Bob Barr (R-Ga.) were shocked that the Administration was refusing to discuss how it was using the power granted to it by Congress under the Patriot Act, frustrating Congress's oversight responsibilities. The Administration has also kept secret, and even denied that it was drafting the Domestic Security Enhancement Act, even after a formal draft was discovered by the Center For Public Integrity in January 2003.

In March 2003, Senator Richard Lugar (R-Ind.) expressed anger at the administration's failure to inform the Congress about the administration's plans to rebuild Iraq. Legislators as diverse as Senator Patrick Leahy (D-Vt.) and former Representative Dick Armey (R-Tex.) have complained in vehement terms about the unprecedented difficulty of extracting information from the administration. Senator John Warner (R-Va.), chairman of the Senate Armed Services Committee, has recently indicated that he would "no longer tolerate the disrespect and secrecy on military matters they've come to expect from the Bush White House."[1] According to Rep. Dan Burton (R-Ind.): "An iron veil is descending over the executive branch that will keep information away from the Congress and the public." An unusual number of other senators and representatives have made similar comments. Of additional concern are claims made increasingly frequently that the White House is using improper means to stifle dissent, among the public, within the government, and in foreign countries. "Lawmakers charge White House with stifling anti-war dissent." (Yahoo.com, March 28, 2003).

Sharing information with the Courts

The Administration has also attempted to protect itself from oversight by the courts, through a variety of policies that either enable it to bypass the courts entirely or that immunize its actions from judicial review. Examples include bypassing Article III courts by unilaterally designating a person — citizen or non-citizen — as an enemy combatant; bypassing warrant requirements by unilaterally indicating that a "significant purpose" (rather than the "primary purpose" under the old law) of the wire tap is related to foreign intelligence; and precluding judicial review and oversight of matters relating to the status of people in criminal and immigration proceedings.

These activities gnaw at the basic assumptions about the public's need for information in a democratic system of government. They challenge the assumption that government should be open to inspection by the public and that citizens — merely by virtue of their inclusion in the polity — have a right to know how the government works.

No Need to Balance

Many people are now talking about the need to balance our interests in national security against our constitutional values. Many people believe that September 11 has shown us that we need to give up some of those values in order to protect our national security. In fact, this analysis presents false dichotomy. The framers would not have presented us with a constitution that would leave us vulnerable to threats of violence. What good would such a constitution be? Nor would the constitution have lasted 200 years — through internal and external attacks, through Civil

War, and more — if it did not protect our national security.

In fact, the constitution, as it is written and as it has been interpreted by the Supreme Court, does not require us to take sides. Nothing in the constitution requires absolute openness at all times under all circumstances. Conversely, nothing in our recent experience justifies blanket secrecy.

The key lies in two basic principles to which the Court has consistently adhered. The first is that, if we are to have a responsible electorate and an accountable government, information about the government must be presumptively available to the public. The second is that when the government *needs* to protect information from public disclosure, it may do so, but only on particularized — and judicially reviewable — findings. *See e.g. Press Enterprise v. Superior Court* (1986) (requiring particularized findings to justify closure of a criminal trial); *Nixon v. U.S.* (1974) (allowing *in camera* review of sensitive White House documents and tapes).

Blanket and unilateral secrecy is inimical to an open democracy. But withholding of certain limited information on a specific and targeted basis may be justified when it is supported by evidence that can be tested in court. Protection of national security demands nothing more; protection of our system of government permits nothing less. In invalidating the blanket closure of certain removal hearings, the Sixth Circuit recently adopted this approach:

> While we sympathize and share the Government's fear that dangerous information might be disclosed in some of these hearings, we feel that the ordinary process of determining whether closure is warranted on a case-by-case basis sufficiently addresses their concerns. Using this stricter standard does not mean that information helpful to terrorists will be disclosed, only that the Government must be more targeted and precise in its approach. Given the importance of the constitutional rights involved, such safeguards must be vigorously guarded, lest the First Amendment turn into another balancing test. *Detroit Free Press v. Ashcroft*, (6th Cir. 2002).

Within the realm of national security, the executive has virtually unchecked power. Neither the courts nor Congress, nor the people have access to the kind of information or enjoy the degree of deference that the President wields in the name of national security. The principal check against the President then is in protecting against the unnecessary expansion of what is deemed national security. If the President can unilaterally designate a person to be of "special interest," or a citizen to be an enemy combatant, or a record to be related to national security and therefore beyond public scrutiny, then he can unilaterally expand the areas in which he can operate without checks.

This implicates not only first amendment values, but the most fundamental constitutional value of all: that of limited government. As Justice Frankfurter wrote about President Truman in his concurrence in *Youngstown Sheet & Tube Co. v. Sawyer* (1952): "It is absurd to see a dictator in a representative product of the sturdy democratic traditions of the Mississippi Valley. The accretion of dangerous power does not come in a day. It does come, however slowly, from the generative force of unchecked disregard of the restrictions that fence in even the most disinterested assertion of authority." ◆

Footnotes:
References available upon request. Contact editorial@mediatwo.com.

J. Patrick Kelly

THE INTERNATIONAL LAW OF FORCE AND THE FIGHT AGAINST TERRORISM

In the aftermath of the terrible tragedy of the September 11, 2001, attack on America, the U.S. government has taken several aggressive steps to fight international terrorism. In only 18 months the United States has launched a major, continuing land and air war in Afghanistan that has toppled the government and embarked on a large-scale attack on the Iraqi government for the purpose of regime change. These actions raise serious and controversial questions of international law that have engaged international lawyers, editorial writers, religious leaders, and even the most practical of people in contentious debate.

I will examine the international legality of the attack on Afghanistan and the more recent invasion of Iraq under both the traditional international law of the use of force and under alternative legal approaches offered by the U.S. government and by international theorists to justify these actions. In a time of international tensions threatening the vital interests of states and of humanitarian disasters like Kosovo and Bosnia, the international community must find alternative ways beyond traditional formal legality to legitimize necessary actions to preserve order and stop the genocidal slaughter of innocents. This search for means may well be the major struggle of the next several decades.

President Bush announced the formal legal justification for the U.S. attack on Al Qaeda in Afghanistan and the Taliban regime on the night of September 11. "We will make no distinction between the terrorists who committed these actions and those who harbor them."[1] In a subsequent letter to the United Nations Security Council the U.S. justified the attack on Afghanistan as based on the right of self-defense because the Taliban permitted parts of its territory under its control to be used as a terrorist base of operation for Al Qaeda.[2] Inherently this is a claim that a state has a right of self-defense after a terrorist attack against any state "harboring" those terrorists.

In the case of Iraq, the U.S. government has not attempted to justify the use of force on the basis of Iraq harboring terrorists. Rather the Administration has offered two distinct justifications for the use of force to remove the regime of Saddam Hussein: (1) several U.N. Security Council resolutions including the recent 1441 authorize the use of force to enforce 'material breaches' of Security Council resolutions; and (2) a preemptive attack on a dangerous regime possessing weapons of mass destruction (WMD) is justified under an expanded doctrine of self-defense.

The Traditional Law of the Use of Force

Since its inception in 1945, the Charter of the United Nations has been the authoritative statement of the law of force. Article 2(4) of the Charter prohibits the use or threat of use of force. This formulation was intended to minimize violence and authorize force only under the collective responsibility of the Security Council. The one exception to this framework was the explicit preservation in Article 51 of "the inherent right of individual or collective self-defense if an armed attack has occurred against a member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."[3]

The traditional view has been that absent specific authorization from the Security Council, attacks or reprisals against states "harboring" terrorists are only justifiable constituting self-defense. The right of self-defense has long been subject to the limitations of "necessity" and "proportionality." The traditional definition of necessity in self-defense, used by the United States and the international community in the Nuremberg trials, is drawn from the *Caroline* incident of 1837.[4] Canadian rebels used the US flag ship *Caroline* to supply their insurgency against the British government in Canada. The British sent a force across the border and attacked the ship killing one American. They then set fire to the *Caroline*, and sent it adrift down the Niagra River where it plunged over the Falls. The British government justified this incursion under the doctrine of self-defense. US Secretary of State Daniel Webster protested this violation of our territorial sovereignty in a letter to the British Ambassador that has become the reigning definition of the concept of 'necessity' in self-defense. Necessity means "instant, overwhelming, leaving no choice of means and no moment of deliberation." The British subsequently agreed with the U.S. analysis of the principles of international law. This high standard permits a response during an attack or when one is imminent, but suggests that once an incident is over and there is time for deliberation the matter should be referred to the Security Council. The purpose of this limitation is to minimize violence and stop the escalation of war.

Several authors have argued for an extended theory of self-defense that would include reprisals to prevent future attacks. The argument is that the pre-Charter right of reprisal survives the Charter or is merged into the concept of self-defense. Preventive self-defense or anticipatory self-defense has some appeal in a dangerous world. But this idea was rejected in both in the UN General Assembly Declaration on Aggression,

which passed unanimously, and by the Security Council's response to the 1985 Israeli attack on the PLO Headquarters in Tunisia. Israel justified the attack as an act of self-defense against a state that was knowingly "harboring" terrorists that had targeted Israel. The Security Council rejected the claim by a vote of 14-0 with the US abstaining. Up until Sept. 11, the international community appeared to reject the concept of preventive or anticipatory self-defense at least until there is an overt act that demonstrates that an attack is imminent.[5]

An additional concept necessary to understand the legal situation facing the United States is that of the customary law of state responsibility. In what circumstances is a state like Afghanistan responsible for the actions taken by non-state actors like Al Qaeda within its territory? Based on a review of state practice including the decision of the International Court of Justice in the *Nicaragua* case[6] and the International Criminal Tribunal for the former Yugoslavia's decision in the *Prosecutor v. Tadic*,[7] the International Law Commission (ILC) summarized the law of state responsibility for actions of a non-state group within a territory. A State is responsible (1) if the person or group of persons is in fact acting under the instructions or control of that State; (2) if the person or group of persons is in fact exercising elements of governmental authority in the absence or default of official authorities; and (3) if the State acknowledges and adopts the conduct in question as its own.[8] At this time there do not appear to be facts on the public record that would support any of those theories. Nevertheless, the Bush administration's 'harboring' theory would impute responsibility to a state that permits a terrorist organization to operate and train within its borders even without supporting or adopting its actions.

The second traditional legal justification for the use of force is authorization by the United Nations Security Council under Article 42 of the Charter.[9] The Security Council may authorize the individual or collective use of force to restore international peace and security by a vote of at least nine of the fifteen members of the Security Council including the concurring votes of the five permanent members: the United States, United Kingdom, France, China, and Russia. After Iraq invaded Kuwait in 1990, the UN Security Council passed resolution 661 under Article 41 mandating economic sanctions and resolution 678 under Article 42 authorizing member states "to use all necessary means to uphold and implement resolution 660 and all subsequent resolutions." "All necessary means" has become the diplomatic language for authorizing force.

Emerging Approaches to the War in Afghanistan

Since the Security Council did not specifically authorize the use of force by the United States in Afghanistan, the U.S. action might be seen as violating traditional notions of formal legality. Nevertheless subsequent Security Council actions and the world's reactions to the events of September 11 may be seen as ratification of the U.S. action and a change in the law of self-defense with regard to states harboring terrorists.

UN Security Council resolution 1373 decides that all states shall prevent terrorists from using their territory for terrorist purposes and deny safe haven to those who finance, or plan, or facilitate terrorist acts. While this resolution does not authorize the use of force as a remedy, it does impose an obligation on states to not harbor terrorists that goes beyond the customary law principles summarized by the ILC. The resolution, in unmistakable language, supports the United States' inherent right of individual and collective self-defense in light of the known fact that the United States was planning to invade Afghanistan to find and capture bin Laden and his Al Qaeda network associates. While the resolution does not specifically authorize the use of force as it did in the Gulf War, it does appear to acquiesce and therefore legitimize US plans to attack Afghanistan as part of an exercise of its right of self-defense. United Nations acquiescence appears to be the appropriate interpretation here because all permanent members of the Security Council are part of the coalition, including Russia and China, and no resolution has been introduced asserting that the United States is in violation of its international legal obligations. The Organization of American States and NATO similarly passed resolutions supportive of the United States right of self-defense in the circumstances.

The Security Council resolution and its subsequent actions indicate that the Security Council approves of and supports U.S. actions in Afghanistan in furtherance of its right of self-defense. This became more clear after Kabul fell. The United Nations and the United States developed plans for a new multi-ethnic government and the long-term process of nation building. The U. N. Security Council unanimously passed a resolution authorizing troops to maintain law and order and endorsing an initiative to form a multiethnic transitional government in Afghanistan.

One could persuasively argue that the United Nations acquiescence and the reaction of other nations have expanded the concept of self-defense to include the use of force against States harboring terrorists. UN resolution 1373 might be seen as approval of an expanded theory of state responsibility attributing the behavior of non-state terrorists to a state that knowingly "harbors" terrorists and does not take action to prevent further terrorist attacks. The United Nations resolution, the continuing role of permanent members of Security Council in the coalition, and the expected United Nation's role in peacekeeping and nation building may be seen as United Nations approval of the removal of the Taliban. The law of state responsibility now appears to include states that are aware of ongoing international terrorism in their territory and who fail to suppress it by refusing to arrest, prosecute, or extradite. Under this interpretation, acts of self-defense would be justified against not only Al Qaeda, but the Taliban government of Afghanistan.

On the other hand, one could also argue that the Security Council approval of the U.S. right of self-defense in these circumstances is *sui generis*. Rather than extend the law, it may be read as constituting only political approval in unique circumstances. I do not think this is a tenable interpretation, but confirmation awaits future events. If Al Qaeda were to attack another country causing a large loss of life from a different base country, I think that the Security Council response would be similar.

The Iraqi War and International Law

Whatever the policy merits of invading Iraq, the above analysis suggests that the legality of the attack on Iraq is more problematic than the ongoing war in Afghanistan. The right of self-defense in Article 51 requires a prior armed attack, and there is, at this juncture, inadequate evidence that Iraq participated in, planned, or financed the attacks on the World Trade Center or

the Pentagon. Nor is there public evidence that the regime of Saddam Hussein has been harboring the terrorists who did.

Some have argued that the Iraqi war like the Kosovo case is an example of a formally illegal action without prior Security Council approval that is nevertheless or will be seen to be legitimate.[10] Yet at this point neither world opinion nor subsequent actions by the Security Council can be said to have legitimized this war. When the United States attempted to secure authorization from the Security Council, three permanent members were announced against the action and more members opposed than supported the measure. At this writing there is broad disapproval rather than approval of the war both in the Security Council and the General Assembly. In a special weekend session of the Security Council prior to the commencement of the war in order to hear the views of nations that were not on the Security Council, there was overwhelming opposition including the representative of the European Union and the Organization of African Unity.[11] Future United Nations resolutions or actions may ratify the U.S. invasion as arguably occurred with regard to Afghanistan and Kosovo, but this appears unlikely at this point.

The Kosovo case is in many respects different. One might argue that even though the U.S. and NATO action in Kosovo lacked the formal legality of Security Council approval, it was nevertheless legitimate because it had the overwhelming support of the international community and was later effectively ratified by the United Nations Security Council. The United States did not seek Security Council authorization because it was apparent that Russia with its long historical ties to Serbia and perhaps China would veto an authorizing resolution. Instead the U.S. and its allies choose to proceed through the regional organization, NATO, which authorized and conducted a NATO operation.

Despite the Russian opposition there was overwhelming support both in the Security Council and the General Assembly for NATO's action to prevent an expansion of this ongoing humanitarian disaster of the systematic murder and rape of innocent Kosovars. Even NATO's rather tardy action would not have occurred without Milosevic's unchecked brutality in Bosnia and Croatia. By a vote of 12-3 the Security Council rejected a draft resolution introduced by Russia condemning the bombing campaign as a violation of international law. In resolution 1244 adopted in 1999 after the NATO bombing campaign, the Security Council welcomed the political settlement and the "international armed presence."

The Kosovo intervention had broad international support, was authorized at least by a regional multilateral institution that placed some check on self-interested unilateralism, appeared to be ratified by the UN Security Council, and was undertaken to relieve an international humanitarian crisis at a time of imminent necessity. These criteria of subsequent legitimation and necessity arguably more than satisfy concerns about its formal legality. In the Iraqi situation there was and continuous to be broad opposition in the Security Council and the General Assembly; strong opposition in NATO; and no humanitarian crisis that demands immediate action to forestall genocidal slaughter.

One must look elsewhere to justify the attack on Iraq. First, the United States and Britain have argued that this use of force is justified under prior Security Council resolutions particularly the recent 1441, finding Iraq in "material breach" of prior resolutions, and resolutions 678 and 687 of 1991 that authorized the use of force to expel Iraq from Kuwait and declared the terms of the cease-fire. Resolution 1441, approved unanimously by the Security Council, does not authorize the use of force or specify a remedy for a material breach of resolutions. The practice of the Security Council has been to specifically authorize members states to use force by the precise words "all necessary means." This specific language was used in the resolutions to authorize force in the Iraqi Gulf War, Bosnia, Somalia, Rwanda, and Haiti. The original draft of resolution 1441 submitted by the US and the United Kingdom would have authorized member states "to use all means necessary to restore international peace and security," but it failed to garner the support of other members.

What 1441 does do is to decide that Iraq remains in material breach of prior resolutions, gives Iraq a final opportunity to comply with its disarmament obligations, sets up an enhanced inspection regime, and decides that the Security Council will remain seized of the matter. Paragraph 12 of 1441 decides that the Security Council will convene immediately to consider remedies if there is a violation of the inspection regime. The decision on the appropriate remedy remains with the Security Council.

The U.S. and British governments have argued that Iraq's material breaches revive the authorizations of force contained in the Gulf War resolutions 678 and 687. The argument is that 687 suspended but did not terminate the authority to use force. 687 does not, however, make the cease-fire conditional upon Iraq's continuous disarmament in perpetuity, but rather on its acceptance of the terms of the cease-fire. The determination of the appropriate remedy for a material breach remains with the Security Council. Paragraph 34 specifically states that the Security Council decides to remain seized of the matter and "to take such further steps as may be required for the implementation of the present resolution...." The decision to use force as a remedy for a material breach of other resolutions is a multilateral matter not one for individual nations to decide on their own. Any other meaning would be a prescription for disaster since all members, not just the United States, are authorized to use force to restore international peace and security. Under such a rationale Russia, Turkey, China, and Iran could all undertake conflicting actions that they deem necessary to enforce resolutions. For good or ill resolutions 678 and 687 were designed to push Iraq out of Kuwait not to remedy the failure to disarm or support regime change.

The Bush administration's second justification has been a claim of an independent right to attack Iraq as a preemptive act in self-defense. As discussed above, Art. 51 of the Charter does support a right of individual or collective self-defense "if an armed attack has occurred." While the advent of nuclear weapons and WMD may require some elasticity in the doctrine of anticipatory self-defense, the *Caroline* case, the experience of domestic criminal law, and common sense require a clearly identifiable, imminent threat as well as proportionality as limits on the use of force. Even under a theory of anticipatory or preventive self-defense, there does not appear to be any evidence of imminent threat of an armed attack on the United States by Iraq. Iraq apparently does not possess nuclear weapons nor does it have the means to deliver nuclear weapons or other WMD to the

United States. For a number of years Iraq has been surrounded by U.S. and British armed forces, and its northern and southern areas patrolled as no-fly zones. While it is likely that Saddam Hussein has hidden biological and/or chemical weapons, it does not follow that they are an imminent threat to the United States. Many states including India, Pakistan, North Korea, Russia, France, as well as the United States, possess nuclear weapons of mass destruction. The United States has even weaponized several dangerous biological agents. The present rules of self-defense do not permit the use of force against states deemed unfriendly or dangerous in order to deny them weapons possessed by many nations. Nor is an armed attack to overthrow a regime necessarily the wisest remedy for possession of WMD.

Does the Bush administration really wish to create a new legal principle that preemptive actions to forestall the future use of WMD is an acceptable form of self-defense? Such a principle would gut the international limits on the use of force and encourage violence, not prevent it. Do we wish to legitimate a Pakistani attack on India or a Chinese attack on North Korea? Such a principle encourages rather than discourages the first use of weapons and could well begin a cycle of violence rather than remove a risk.

The United Nations was created after World War II to outlaw the use of force and to construct a system of collective self-defense to discourage unilateral and subjective justifications for war. This system and our standing in the world are in peril. Saddam Hussein was a murderous tyrant who used chemical agents on the Kurdish Iraqis. His removal should be beneficial for the Iraqi people and world peace. Yet the U.S. government's unilateral means and dismissive tactics toward even allies has antagonized normally supportive governments and outraged hungry and desperate people on all continents. Such an unilateralist ap-proach creates resentment and becomes an impediment to necessary international cooperation.

U.S. security and indeed our prosperity are dependent on our engagement and multilateral cooperation with the nations of the world. We are dependent on other nations for military intelligence necessary to prevent future terrorist attacks. Foreign intelligence led to the penetration of cells in France and Italy that prevented attacks on US in-terests in Europe. Both ours and the world's prosperity are dependent on the ongoing cooperation to keep open the shipping, transportation, and communications channels that are necessary for international commerce. As lawyers, we understand that it is the web of international trade institutions and rules that form the facilitative framework vital to economic growth and development.

This is an uneasy time for international law and the institutions created after World War II. The rules designed to discourage war and to minimize violence are themselves under attack. A wise reconstruction of a viable international legal order remains to be seen. ◆

Footnotes:

References available upon request. Contact editorial@mediatwo.com.

Mike Kelsey

THE USA PATRIOT ACT: COMPLIANCE WITH THE ANTI-MONEY LAUNDERING PROVISIONS

What do banks, gem dealers, mutual funds, travel agents, securities brokers and auto dealers have in common? These industries and many others have seen new anti-money laundering (AML) laws become part of the way they do business. Signed into law on October 26, 2001, the USA Patriot Act ended years of debate on expanding or limiting the scope of AML laws in American commerce. This article reviews how the Patriot Act has changed the anti-money laundering compliance landscape.

Pre-September 11 Money Laundering Regulation

In 1970 Congress enacted the "Bank Secrecy Act" ("BSA"), the United States' primary anti-money laundering statute. In an era when drug traffickers and organized crime were law enforcement's primary financial crime targets, BSA regulations focused largely on cash transactions, establishing a reporting and record keeping system to help law enforcement track the movement of cash. The most familiar of these reports is the Currency Transaction Report ("CTR"), which requires banks and other financial institutions to report cash transactions exceeding $10,000 with the Internal Revenue Service. Other original BSA requirements include logs of cash purchases of monetary instruments and reports of cross-border cash activity.

These requirements dealt with the "placement" stage of laundering, when illegally obtained currency is first inserted into the financial system. Although the BSA defined financial institutions to include a wide range of industries, in these early years banks and thrifts were seen as the most likely location for placement. Regulations issued by federal banking agencies required these depository institutions to establish internal controls and compliance programs that ensured the timely and accurate filing of CTRs.

Unusual transactions could be noted as "suspicious" on CTRs by checking a box on the form, or separately reported on "criminal referral forms" used for advising law enforcement of illegal transactions conducted through the bank. These suspicious reporting methods were usually used to flag cash transactions that were changed or maintained just below the CTR filing threshold, a process known as "structuring." Little attention was given to other industries that fell within the "financial institution" definition (such as travel agents, pawn brokers and gem dealers) or other types of transactions (such as wire transfers).

For many years following the enactment of the BSA, banks and thrifts that properly filed CTRs and maintained other records usually were found to have adequate compliance programs under regulatory examination guidelines. There was little enforcement of the BSA upon other financial institutions that were subject to the BSA, nor did regulators focus on the "layering" or "integration" stages of money laundering, which occur when criminals move placed funds among financial institutions to disguise it, or invest it into commercial activities to make it appear legitimate.

Eventually it became clear that most criminals using the financial system were well aware of the almost exclusive emphasis on cash placement in BSA regulation, and to avoid detection used alternatives to place their illicit cash, such as smuggling it to countries that had weak anti-money laundering laws, or purchasing multiple monetary instruments (such as postal money orders) at domestic sources, a process known as "smurfing." The government determined that the cash reporting and record keeping elements of the BSA needed to be supplemented with additional measures that covered other types and stages of money laundering. In the 1990s, additional regulations required banks to maintain records of wire transfers, and report unusual, unexplained transactions on "Suspicious Activity Reports" (SARs) instead of the "check the box" CTR option. Implicit with the introduction of the SAR regulations was the notion of proactive identification of suspicious transactions, where banks actively identify situations where money laundering occurs instead of merely reporting it when they stumbled across it. Bank examiners began to examine the adequacy of these proactive detection processes, moving AML laundering compliance to the forefront of bank compliance concerns.

This momentum reached a peak in 1998 when federal regulators proposed "know your customer" (KYC) regulations that would require banks and thrifts to identify and "profile" customers based on perceived money laundering risks and "monitor" the activities of those who were viewed as especially risky, such as affluent "private bank" customers who often received special treatment. Regulators believed these regulations would assist institutions in understanding the vague expectations of bank examiners in customer identification matters, and enable law enforcement to more easily access banking businesses that had historically been favorites of criminals for hiding illicit assets.

Coincident with the proposed "KYC regulations," however, was the emergence of consumer privacy as a major public

policy and political issue, which eventually would result in expansive federal consumer privacy legislation. This environment was not politically suitable for the adoption of regulations that referenced customer "profiling," and the KYC regulations were withdrawn after thousands of negative comment letters were submitted by privacy advocates and financial institutions.

The withdrawal of the KYC regulations was viewed as a major defeat for supporters of tougher AML laws. American policy makers found it difficult to pressure other governments to toughen their anti-money laundering laws when domestic customer identification regulations were soundly rejected. The Financial Action Task Force ("FATF"), an international organization of nations with common standards in money laundering compliance expectations, began to voice concerns about deficient money laundering laws in emerging capitalist markets and small nations that had traditionally been "tax havens" using strict customer privacy as a lure for international banking business development.

A major scandal brought money laundering to the front page of mainstream American news coverage, when a multi-billion-dollar wire transfer scheme at a major New York bank was exposed. Russian money launderers allegedly used bank insiders to move International Monetary Fund loan proceeds and other funds out of the country and into "tax haven" bank accounts in little known places like Nauru and the Channel Islands. Congressional hearings regarding the scandal featured bank CEOs promising to implement extensive compliance monitoring programs to catch large wires involving problem countries. Software vendors offered complicated monitoring systems to serve these needs, and banks began to see even tougher money laundering exams with examiners demanding the allocation of an ever-increasing amount of compliance resources into suspicious transaction detection programs. Around that time, the General Accounting Office released a report that suggested Russian organized crime was using Delaware corporations and United States bank accounts to launder billions of dollars of assets, noting that none of the parties involved was doing any inquiry into the identity of the foreign parties.

Following these incidents, regulators and law enforcement argued that traditional CTR reporting failed to detect high-risk wire transfers and other fund movements. Also of concern were deficient foreign jurisdictions whose poorly regulated banks had correspondent relationships with American institutions, allowing foreign persons indirect and usually undisclosed access to the United States banking system. Equally troubling was the perception that criminals were leaving domestic banks and taking their laundering to other players in financial services, such as mutual funds, insurance companies and money transmitters, who were considered much less sophisticated in their compliance efforts and were, in many cases, unregulated for AML compliance.

This was the AML landscape on September 11, 2001. Banks were developing their compliance programs and focusing on the identification and reporting of large transactions involving "high-risk" countries, as well as meeting their traditional cash reporting requirements. Without new legislation or regulations, regulators were increasing their scrutiny on banks and thrifts with new examination guidelines that lacked consistency. Other players in the financial industry saw some increased interest in anti-money laundering by their regulators, but few new regulations were issued to formalize this oversight. And the public focused more and more on their privacy rights as they began to receive privacy notices from their financial institutions.

The USA Patriot Act

September 11 changed American life in countless ways, and assumptions of American invulnerability were replaced with doubts about law enforcement and intelligence capabilities. Immediately after the terrorist attacks, banks began to question their AML compliance measures as they discovered the existence of accounts opened by the September 11 hijackers to finance their activities. They concluded that their expensive large transaction monitoring programs failed to flag the relatively small wire, cash and ATM transactions of the hijackers. They learned that their account opening procedures often allowed customers to use falsified documents without detection. And as details about the banking habits of the hijackers were published, their reputations suffered, even though they had not violated any laws.

The reputations of law enforcement and intelligence agencies also were damaged. Besides suggestions that some agencies ignored warnings regarding unusual flight school and other leads, it was leaked that a bank used to move funds for leader Mohammad Atta had filed a SAR after receiving a $100,000 wire transfer. These funds were then distributed to other bank accounts throughout the United States. Law enforcement evidently did not follow up on the case, leading some to conclude that another missed opportunity had occurred to catch the hijackers before the attacks. Of course, it is unlikely that the Atta SAR had any aspects that would have made it stand out among the over 200,000 SARs that were filed in 2001.

In the weeks following September 11, Congress and the Bush Administration brought together many security issues into a single piece of legislation that became the "USA Patriot Act." It included a major overhaul of the nation's anti-money laundering laws, adding many new compliance requirements for traditional financial institutions, and expanding the coverage of these laws to many other businesses. In a sense, the money laundering section of the Act took all of the proposed ideas to toughen anti-money laundering and made them law, with some new ideas for combating terrorist financing tossed in. Seemingly impatient with the slow progress in establishing new requirements for some financial institutions over the years, Congress imposed extremely short time frames for Treasury and other regulators to issue new regulations under most parts of the Patriot Act. When the Act was signed into law on October 26, 2001, the nation's financial services industry was served with what is arguably the most aggressive and comprehensive set of new compliance requirements in memory.

It would require a dedicated issue of the *Delaware Lawyer* to review all of the AML provisions of the Patriot Act. There are important changes to the asset forfeiture laws that should be reviewed by lawyers who advise commercial clients or financial institutions that have international commercial activities. There are also employment law issues dealing with the ability of a financial institution to advise a potential employer of a former employee's suspicious activities. Instead of evaluating each section, we will review some key provisions of the Act that expand the application of the nation's anti-money

laundering laws to non-bank financial institutions and other persons, and then cover important new compliance responsibilities that apply to all persons now covered by these laws.

Extended Application of Bank Secrecy Act

When the BSA was enacted in 1970, Congress understood that despite the dominant role the depository institutions banks and thrifts played in the American financial system, there were other types of financial institutions that could be used to launder money. The threshold definition of "financial institution" contained in the BSA originally included securities broker-dealers, mutual funds, money transmitters and insurance companies as well as the depository institutions. However, despite this broad statutory coverage of the BSA, only those institutions whose regulators enacted specific regulations were required to adopt formal anti-money laundering programs or, more recently, file mandatory referrals of suspicious transactions with law enforcement.

Except for occasional efforts by the Financial Crimes Enforcement Network (FinCEN, a bureau of the Treasury Department responsible for various aspects of money laundering regulation, including the direct regulation of BSA-defined financial institutions not subject to examination by federal banking or securities regulatory agencies) there was little meaningful regulation of non-bank institutions. This created an uneven playing field within the financial services industry, triggering concerns from the depository institutions regarding unfair compliance burdens, and law enforcement concerning the migration of money laundering into poorly regulated industries.

In the months leading to September 11, FinCEN began to take long-awaited action with respect to some elements of the financial services industry that were considered especially vulnerable to money laundering. These included "money service businesses" who process fund transfers, cash checks and provide other services for people without bank accounts. FinCEN adopted regulations requiring the registration of these businesses and the adoption of basic anti-money laundering programs. Other FinCEN initiatives included proposed regulations requiring securities brokers to file SARs. Most other types of institutions, such as mutual funds and insurance companies, had few formal compliance expectations comparable to the laws governing depository institutions.

The Patriot Act leveled the playing field of AML compliance by essentially raising the bar for all entities that fall within the "financial institution" definition. Congress showed its impatience with FinCEN and other federal agencies by requiring Treasury to issue AML program regulations by April 24, 2002 for institutions that are regulated by a federal banking or securities agency. These regulations proposed formal requirements for mutual funds, credit card servicers and money service businesses, and confirmed the coverage of banks, thrifts, broker-dealers, casinos and commodities futures merchants. While there are some differences among the regulations, they all require covered institutions to appoint an AML compliance officer, adopt relevant policies and procedures, train employees, and independently test the adequacy of the program, which had to be documented and approved by the board of directors. These regulations were effective on July 24, 2002.

Congress, however, went an important step further with the formal AML program requirements. Treasury was instructed to issue AML program regulations by October 24, 2002 for businesses such as precious metals dealers and pawnbrokers that fell within the definition. While Treasury used its statutory authority to defer the issuance of some of these regulations, proposed regulations or notices of proposed rule making have been issued for certain types of investment and insurance companies, gem dealers, travel agents, car dealers and other businesses. These proposed regulations try to balance the relative risks of money laundering against the compliance burdens the programs would raise. For example, in the insurance area, companies such as property and health insurance were viewed as having no potential money laundering risks, as were some types of investment companies that limit shareholder redemptions. In cases where money laundering risks were seen, the proposed regulations would require the same formalities (AML compliance officer, employee training, etc.) that applied to banks and other traditional financial institutions.

An interesting approach towards dealing with "underground banking systems" (such as the Halwa currency exchange practice common in the middle east) is Section 359's inclusion of them in the "money services" industry, thus requiring registration with FinCEN and all the requirements that pertain to this industry, such as SAR filings. While it seems far-fetched to presume that any underground system would comply with federal AML laws, this section was probably intended to provide tools for federal law enforcement and prosecutors to charge these systems with crimes when they were detected.

Besides specific AML program requirements, the Patriot Act required federal agencies to report to Congress on some high-risk money laundering issues. For example, Section 356 required a combined study by Treasury, Securities the SEC and Federal Reserve on the money laundering risks of investment companies and whether "personal holding companies" (investment companies owned by four or less people) warranted "financial institution status" under the BSA. The agencies reported that the regulatory process being established by issued regulations governing mutual funds and other investment companies adequately dealt with money laundering risks and, much to the relief of investors and the institutions they deal with, declined to recommend "institution" labeling for the private holding companies.

Another mandated study pertained to reducing CTR filings. It is a generally accepted notion that the vast majority of the millions of CTRs filed annually have no law enforcement utility, and needlessly tie up public and private resources that would be better used focusing on higher-risk activities. Many banks fail to fully utilize CTR filing exemptions available for retail and stock exchange business customers, simply because the complexities (and potential penalties of mistakes) of some of the exemptions make it more cost effective to file CTRs for all reportable transactions. Treasury's study (conducted through an independent accounting firm) recommended that the exemptions be modified to encourage widespread use, perhaps by easing some of the technical requirements. However the $10,000 filing trigger, unchanged since the enactment of the BSA in 1970, remains in place.

Congress also required Treasury to report on the challenges faced by institutions in verifying the identity of foreign nationals with accounts at United

States institutions. It came as no surprise when this study reinforced what banks and other financial institutions had known for years: the verification of the identity of a foreign customer was a difficult if not impossible task. This study was relevant to some of the major substantive additions to the nation's anti-money laundering laws applicable to both the traditional and new types of businesses with AML compliance responsibilities, and confirmed that there were limits to what a financial institution could reasonably do in the hunt for terrorist funding.

New AML Requirements

Besides expanding the coverage of AML compliance into new industries, the Patriot Act adds many important substantive compliance responsibilities, especially with respect to foreign customers of financial institutions. Within 60 days of its signing into law, the Act required banks and securities brokers to close all accounts maintained by foreign "shell banks," which are banks that have no physical presence in any country and are not affiliated with physically identifiable and regulated banks. The shell bank matter was viewed as an urgent issue, since it was thought that such banks allowed money launderers and terrorists to use their correspondent accounts at United States banks, and that some of these banks may actually be owned by criminals. The "guidance" that introduced this requirement under Section 313 of the Act included a "safe harbor certification" that could be completed by the foreign correspondents of United States institutions to confirm that they were not shell banks, did not allow shell banks to use their US account, provide information concerning their ownership, and indicate a United States agent for service of process.

Subsequent regulations issued eased the compliance burden of the certification process by allowing a holding company to certify all of its foreign banks with a single safe harbor certificate. In perhaps an unintended consequence, this section also swept foreign branches of United States banks into the "foreign bank"' definition, creating a somewhat cumbersome shuffling of safe harbor certificates between United States institutions to cover the accounts their foreign branches may have with other domestic banks.

Traditional deposit accounts are relatively simple to identify in the shell bank prohibitions under Section 313. However, the definition of "account" is very broad, contemplating literally any type of financial relationship between a foreign bank and a United States institution, not all of which fit easily into the certification process. For example, a reasonable reading of the regulations suggests that a loan participation, where a foreign bank purchases an interest in a complex domestic commercial loan transaction, could be a "correspondent account" subject to the certification requirement. However, it is unclear what action, if any, a United States bank could take opposite an established participation if a foreign bank failed to provide one for a preexisting deal.

As a practical matter, many banks believe the bank-by-bank certification requirement, even if holding company level certifications are obtained, triggers unnecessary paperwork when prominent foreign financial institutions based in countries with strong AML laws have to provide certifications to thousands of United States banks and broker-dealers. It could be argued that a better approach would be for the federal government to maintain a list of acceptable banks that could maintain correspondent accounts without separate certifications (similar to the list of "bad" banks included in the list of Specially Designated Nationals and Blocked Entities maintained under laws administered by the Office of Foreign Assets Control), enabling institutions to focus on banks that may have a greater risk of money laundering and terrorist financing.

Congress added additional compliance requirements opposite foreign financial institutions in Section 311, raising the notion of "expanded due diligence" for accounts maintained at United States institutions by financial institutions from countries with weak anti-money laundering laws. In March 2001, proposed regulations for the banking and securities industries set forth a complicated process for determining what foreign institutions had to provide detailed information about their anti-money compliance programs in order to maintain an account with a United States institution. Of particular concern were "payable through" accounts, where foreign banks allow its own customers to use its United States account on an undisclosed basis. Such accounts would be banned for banks from high-risk jurisdictions.

Section 311 also deals with corrupt foreign government officials who might use a United States account to launder stolen funds. "Private bank" accounts (defined as accounts with a $1 million minimum asset requirement) maintained for foreign political officials require extra scrutiny to assure that they are not used for illegal purposes. Proposed regulations for this part of Section 311 provided that United States institutions could assume a customer was not a foreign official if they noted on their application they were not, and the institution had no information to suggest that this indication was incorrect. Without a data base that provides reliable information identifying foreign government officials (and their immediate family, also covered) it would appear that complying with this section of the Patriot Act will be difficult for many United States institutions. The regulations proposed under Section 311 were not final as of the date of this article.

Whereas Sections 311 and 313 deal with general concerns about foreign customers, Section 312 adds a specific law enforcement tool against nations whose money laundering policy deficiencies present very serious gaps in global compliance efforts. Section 312 provides Treasury with a choice of five measures that can be applied against such nations, ranging from special record-keeping requirements for United States institutions that have customers from those nations, to an outright ban on correspondent accounts for banks from those countries. In late December 2002, Treasury issued the first measures under this Section, banning correspondent bank accounts from Nahru and proposing significant record-keeping requirements for accounts and transactions from Ukraine. The Ukrainian sanctions were subsequently withdrawn when additional AML efforts were implemented in that country.

Perhaps the most far reaching of all the AML provisions in the Act are the "customer identification program" ("CIP") requirements of Section 326. Resurrecting one component of the failed KYC regulations, Section 326 mandates regulations that require financial institutions to adopt formal customer identification programs. The first round of such regulations apply to banks and other depository institutions, securities broker-dealers, and mutual funds, with more to follow when other financial institutions have formal AML program responsibilities.

What You Should Know About Money Laundering Laws

While lawyers are not "financial institutions" under the BSA (unless they happen to fall within another category, such as a "real estate settlement party"), every lawyer should be aware of several fundamental components of AML laws that could have important implications on their practice:

1. Know Your Client. Lawyers should be aware of the notion of "knowing your client" in the context of unintentional participation in money laundering or terrorist financing schemes, and be cautious of misplaced reliance on the attorney-client privilege in shielding the lawyer from potential prosecution. In assisting a client in such routine commercial functions as incorporating a business entity or negotiating a commercial transaction, lawyers should pay close attention to red flags of money laundering or terrorist financing to avoid unintended complicity in money laundering prosecutions. Conduct basic due diligence into the legitimacy of the client and gain an understanding of the purpose behind each transaction. Failure to do so, especially when basic due diligence would reveal troublesome information, could lead to serious ramifications for the lawyer.

2. Basic BSA Reporting. Lawyers who lower the amount of a cash transaction to avoid a CTR filing, or continually maintain cash activity in a manner to avoid reporting, run the risk of federal investigation or prosecution for "structuring." Even worse would be circumstances where a lawyer assists or counsels a client to avoid CTR reporting. Lawyers may incorrectly think that every CTR triggers a federal investigation. In fact, if a lawyer handles their personal or firm finances appropriately, the filing of a CTR is just one of the millions of records maintained by the IRS. Lawyers involved in international transactions should also be aware of related filing requirements and laws of the countries that may be relevant to their work.

3. Intimidation of Bank Employees. Lawyers who are unaware of currency reporting requirements or the upcoming "customer identification" regulations might balk at giving a bank teller their identification information when requested. In some cases lawyers might incorrectly perceive such requests as "privacy violations" and threaten the teller with legal action. Such threats just demonstrate the lawyer's ignorance of the law. When asked for identification in connection with a financial transaction or account, lawyers should just provide it, even if it is with an institution they have done business with for years.

4. Possible AML Issues for Clients. Lawyers who advise gem, jewelry or car dealers, travel agents, insurance companies and any other business listed as a "financial institution" should pay attention to the AML regulations being issued by the Treasury Department. These regulations could require their clients to establish formal "compliance programs," impose customer identification programs, or mandate SAR filings, similar to banks and other more traditional financial institutions.

5. Discovery of SAR Filings. Financial institutions may never disclose the filing of a SAR, and requests for production that include them should not be obeyed. Institutions that are asked to disclose or produce a SAR are instructed to immediately notify their federal regulator for assistance, and not disclose. There have been embarrassing situations where bank witnesses refuse to answer a question about the existence of a SAR filing in court, triggering awkward exchanges with a judge who is unaware of the prohibition on disclosure. Newspaper accounts of SAR filings by banks are usually the result of inappropriate disclosures by law enforcement agents or prosecutors who incorrectly believe the ban doesn't apply to them. The bottom line is simple: when it comes to SARs, don't ask and don't tell.

The fundamental premise of the CIP regulations is that every new customer (or existing customer that has not been identified that opens a new account) must provide basic identifying information, and the institution must take some action to verify the accuracy of that information. This basic information includes name, address (mailing and, if different, residence or principal place of business), identification number (generally a tax identification number) and, for individuals, date of birth. Once obtained, the institution must verify that information either by observing a document (such as a drivers license, passport or a business document such as a certificate of incorporation) or a back-office process that evaluates the accuracy of the data.

It is anticipated that accounts opened in person would usually include verification by document, and that remote account opening processes (internet, mail, telephone) where visual comparison of a picture of the customer with one on the document would be impossible) would rely exclusively on back-office verification. The verification process must also screen the data against lists of known terrorists and money launderers provided by federal authorities. If derogatory information is obtained in the verification process, the institution must correct it, and in appropriate cases file a SAR.

The CIP regulations essentially mandate processes most banks and broker-dealers have followed for years, where many institutions often employ both document and back-office processes to verify customer information as part of fraud-loss avoidance efforts. The requirements for mutual funds may be more cumbersome to the extent that date of birth has not been traditionally captured as required account opening information. Upcoming industries that will have CIP regulations, (such as travel agents and pawn brokers) may find compliance far more challenging. Perhaps the greatest challenge lies in verifying the identity of foreign customers, because as Treasury concluded in its report to Congress, the verification of information provided by a foreign individual, even by observing a document with a photograph, is extremely difficult, simply due to the lack of reliable data bases to validate information and the availability of falsified documents.

In that regard, for all customers (domestic or foreign) it is important to note that while the verification of the information provided by a customer (e.g. that there is a social security number issued to a person on the customer's date of birth, that a person by that name lives at the provided address, or that the person opening the account resembles the photograph on the document) is in most cases a reasonable expectation, there is no assurance that the customer who presented the information is indeed that person. Indeed, there is speculation that the bank accounts opened by the September 11 hijackers would have been opened even under an acceptable CIP that verified documents. Because of this important limitation of verification capabilities, characterizing the Section 326 regulations as "customer verification" regulations is somewhat of a misnomer.

Among the many other AML provisions of the Act is a very important and controversial "information sharing" section that significantly expands the federal government's ability to obtain customer information from financial institutions and provides a mechanism for financial institutions to share customer information with each other. Regulations under this section allow FinCEN to request information from financial institutions outside of the grand jury or administrative subpoena processes. Starting in February 2003, every two weeks banks, thrifts, broker-dealers and a few other institutions receive e-mails

from FinCEN with names and identifying information of suspected money launderers and terrorists, requiring a search of account and transaction records within 14 days. Intended as a format for addressing urgent matters of national security, there is concern that the process is instead being used by law enforcement agents as an investigation shortcut for less serious crimes.

Section 312 also allows the sharing of information about money laundering and terrorist financing among institutions. In order to share or receive such information, institutions must file a certificate with FinCEN that indicates its commitment to maintaining the security of information it may receive. The sharing institution must confirm that the receiving institution has also filed its certificate, and FinCEN is issuing lists of participating institutions to aid in this due diligence. Oddly, such certificates are also required for sharing information within a holding company (although there may be other legal means of doing so under the Fair Credit Reporting Act). Given the outcry that accompanied the KYC regulations, institutions that file their information-sharing certificates should be prepared for adverse publicity from those who claim that filing the certificate means an institution is compromising the privacy rights of its customers.

A final section of the Act that merits highlighting is the new inclusion of AML compliance as a factor in bank mergers and acquisitions. Section 327 requires the FDIC and Federal Reserve to consider the AML compliance record of banks or holding companies, including their foreign branches, in merger and acquisition applications. Just as a deficient Community Reinvestment Act compliance record can derail a bank merger, so too can an AML compliance problem now have huge business implications.

The Future of AML Regulation

In financial institution compliance, some subjects often take on a "flavor of the month" where one hot issue is eventually replaced by another. Odds are that money laundering will not follow this lead, at least as long as terrorism is a threat to our society and our financial system is used to finance it. By extending AML compliance to commercial businesses such as car dealers, travel agents and gem dealers, it is more likely that AML will grow as an issue and add new costs of doing business for all of them. Perhaps the only concern that could slow the expansion of AML compliance would be public outcry (and political fallout) over privacy concerns, and should terrorism fade as a threat this may very well occur. Indeed, the AML component of the Patriot Act includes a September 30, 2004 sunset provision allowing its termination upon a joint Senate and House resolution to that effect. But unless this unlikely event occurs, American businesses should expect even more AML policy initiatives from Congress and regulatory agencies as the ever-moving targets of money laundering and terrorist financing try to stay one step ahead of detection. ◆

Footnotes:

References available upon request. Contact editorial@mediatwo.com.

STUDENT ESSAYS

Reid-Dixon (Continued from page 28)

making, justices are able to render a more impartial verdict. Rather than viewing defendants as a certain class of people, judges are able to view them as citizens of the United States who are entitled under the Constitution to a fair and impartial trial. Nothing more, nothing less.

Another crucial part in the success of our government as we know it lies in the freedom of the press to discover and transfer information to the American public. If there were no laws protecting the freedom of the press, we would lack the individuality that America represents. With one mainstream idea or way of doing things, people would lose their sense of individual opinion and therefore concede to the majority (whether it be right or wrong) without knowing it. With freedom of the press being an individual freedom protected by the document on which this country is based, we allow for the continued expression of all those who wish to be heard within this country; and accordingly maintain the general acceptance of other cultures, ideas, and beliefs here in America.

Just as a teenager hopes to assert their independent nature by making their own decisions and speaking their point of view, so too does America. The forefathers established a system through which each citizen is able to contribute to this great country through their individuality. And without such fundamental principles as a free press and an independent judiciary, this goal perhaps could not be achieved. Through the cultivation of these ideals, however, America continues to improve every day. ◆

Roark (Continued from page 28)

explaining an opinion and a recent event in the paper or story. Ideas are tossed into the free press arena for anyone to snatch up and learn about.

Free press also protects the ideas of those who don't have a strong majority in government; these ideas are not drowned out by the monopolies. So there is always another view available. People are able to choose which view they agree with or form yet another view based on the information that is available thus new ideas continue to move around. Those once obscure ideas of a minority faction may one day, thanks to free press, become the slogan of the majority. There was no mistake in making freedom of the press, along with the other freedoms Americans hold dear, a part of the first amendment. It is a valuable freedom and resource that allows everyone to be heard.

Free judiciary and free press permit the government to better suit the people it is there to work for. It stops the adulteration of the law and destruction of minority ideas. Democracy would not exist without these two ideas, and I thank the founding fathers for integrating them into the lives and hearts of Americans. ◆

Dobrich (Continued from page 28)

system is based on the policy that twelve guilty people should go free as long as not one innocent person is sentenced. By being free of political or social pressures, judges are able to deliver fair and impartial verdicts of innocence or guilt.

Without this separation of political and social pressure, we would be no better then the dictatorships of other countries. America would not be the impressive democratic nation it is if the judicial branch of the government were based on the pressures of those in political office. America's illustrious glow to foreign nations would not be so bright if it were not for the freedoms and sovereignty that we take for granted. ◆

BAR BENCH MEDIA CONFERENCE ESSAY CONTEST WINNERS

The Bar Bench Media Conference of Delaware, formed in 1975, was designed to develop and foster the mutual understanding essential for conducting fair and impartial court proceedings without encroaching upon the freedom of the press. The Conference consists of representatives of the Delaware electronic and print media, judiciary and legal community. Each year, the Conference sponsors an essay contest for 11th and 12th grade Delaware public high school students on the importance of an independent judiciary and free press. *Delaware Lawyer* is pleased to present this year's winning essays by Erica Reid-Dixon of Caesar Rodney High School in Kent County, Kendra Donna-Marie Roark of Cab Calloway High School in New Castle County, and Samantha Dobrich of Sussex Central High School in Sussex County.

THE IMPORTANCE OF AN INDEPENDENT JUDICIARY AND A FREE PRESS

ERICA REID-DIXON

Every teenager will reach a point in their life in which they feel the need to take control of their future and assert their independence. Teenagers are always trying to branch out from the nest and in essence become a contributing part of society on their own. The ability to say what's on your mind, and make your own decisions are two fundamental values that set the framework of America apart from other systems in the world. This fact is evident in the very pages of the Constitution written by our forefathers to forever protect these personal freedoms. In order for our society to function as was intended, it is essential that a sort of fourth and fifth branch exist in the form of a free press and an independent judiciary. Through free press and an independent judicial system, America is able to function as was intended: to protect minority rights while under majority rule.

An independent judiciary is one that is free of political or social pressures. This is not just a romantic notion that is rarely achieved, but rather, a system that our government actively strives for. What kind of justice would there be if those making the decisions were swept up in public opinion? Why, we would find ourselves back in the year 1692 with the Salem Witch Trials, during which all neutrality and level-headedness was thrown to the wind resulting in the loss of the lives of nineteen men and women. In these cases, the judges felt the pressure of society upon them and were forced into delivering hasty and irreversible judgments upon innocent people. However, we can prevent further judicial wrongs such as those committed in Salem by stressing the importance of an independent judicial system. By removing social and political pressure from the realm of decision

(Continued on page 27)

KENDRA DONNA-MARIE ROARK

An independent judiciary and free press are two important aspects of our government. These two freedoms go hand in hand protecting the people and allowing opinions to be heard.

The idea of an independent judiciary is extremely important. Judges can make decisions based on the law and not fear the social and political backlash, which may ensue. There have been many cases that exhibit this idea. Without an independent judiciary landmark decisions such as *Brown v. The Board of Education* and *Roe v. Wade* might not have been made. Judges were able to look into the facts of the cases and form an opinion; not one forged by social or political pressure but based on the facts of the case at hand as it applies to the law.

Judges have to be able to do their jobs and not worry or fear the consequences if a decision does not fall along with the popular opinion of that time. This is why certain decisions could have been made, even though the decision was contrary to popular opinion. The decisions could be made without the judges worrying about what the popular opinion was, and if they would not be "reelected" for the office again. This concept is able to protect the law and constitution from political and social trends of the day.

Free press provides those who disagree with judicial decisions a platform to speak out against that decision, just as free press allows people to speak for a decision. Ideas are thrown into the open for people to read or hear about. People are able to form opinions with more information as well as get new perspectives on the world around them. Free press allows the average citizen to be heard through articles about what is going on in the city to editorials

(Continued on page 27)

SAMANTHA DOBRICH

Fear is caused by the unknown, the hidden. There is a lot to fear in America as we plunge into war. Fear of biological warfare, fear of our soldiers being subjected to chemical weapons and the fear of what will happen next.

Luckily we live in a country of free will and democracy. Thanks to the freedom of the press, Americans know what is happening at home and abroad and the effect it will have on them. Imagine living in Communist Russia, or under the control of Iraqi officials, never knowing what is going on in the outside world, only knowing what your leaders want you to believe. The allowance of an unbiased press means that information gets to the American people in all shapes and forms. Although some reports may be more accurate then others and the viewpoints at times obscured, it is still information, and more than what citizens in other countries are allowed to have.

The fact that the press consists of ordinary citizens and is not under government control is a big part of what makes America great. You learn the good along with the bad, the right and the wrong. It is difficult to hide government corruption without American knowledge and, believe it or not, the media gives Americans a voice in the running of our government. Political decisions are heavily weighted by public opinions and the news makes sure that the people make their feelings known. The government has no censorship over the news media, allowing the truth to be available to American citizens.

An independent judiciary is just as important to the democratic process as the freedom of the press. Innocent until proven guilty is one of the countless concepts that foreigners admire in the American judicial system. Our judicial

(Continued on page 27)

WHO CAN YOU DEPEND ON TO GET YOUR CLIENTS BACK TO WORK?

Depend on us to get you better faster.

GETTING YOUR CLIENT BETTER FASTER!

BOARD CERTIFIED PHYSICAL MEDICINE AND REHABILITATION SPECIALISTS

A MULTI-SPECIALTY TEAM DEDICATED TO TREATING YOUR CLIENT'S PAIN WITH NON-SURGICAL CARE & REHABILITATION

ACCEPTING NEW MOTOR VEHICLE & WORKERS COMPENSATION CASES

Physical Medicine / Rehabilitation / EMG

Barry L. Bakst, D.O.
Craig D. Sternberg, M.D.
Arnold B. Glassman, D.O.
Anne C. Mack, M.D.
Stephen M. Beneck, M.D.
Susan T. Depoliti, M.D.
Asit P. Upadhyay, D.O.

Pain Management Counseling

Irene Fisher, Psy.D.

Chiropractic Care

Kristi M. Dillon, D.C.
Brian S. Baar, D.C.
Debra Kennedy, D.C.
Kenneth Ward, D.C.
Mary B. Beierschmitt, D.C.
Marjorie E. MacKenzie, D.C.

Interventional Pain Management

Ginger Chiang, M.D.
Emmanual Devotta, M.D.
Pramod K. Yadhati, M.D.

Depend on Teamwork for: Physical medicine & rehabilitation, Interventional Pain Management / Injections, EMG, Chiropractic Care, Rehabilitation therapy, Psychology / Pain management counseling, Massage therapy and QFCE's

Depend on Time Saving Solutions: Centralized communication — we'll keep track of every phase of your clients' care. Prompt scheduling — often within 24 hours. Timely response — to your requests for documentation. One call — for any record requests.

Depend on Convenience: Five convenient locations. Hospital consultations at St. Francis, Christiana Care and Kent General. Early morning, lunchtime and early evening appointments. Free, handicapped accessible parking. Transportation provided for auto, work and personal injury. Accessible to public transportation. ONE STOP SHOPPING!

GETTING YOUR CLIENTS BETTER FASTER IS JUST A PHONE CALL AWAY. CALL US TODAY!

Wilmington

2006 Foulk Road
Wilmington, DE 19810
302-529-8783

700 Lea Boulevard
Wilmington, DE 19802
302-764-0271

Newark / Glasgow

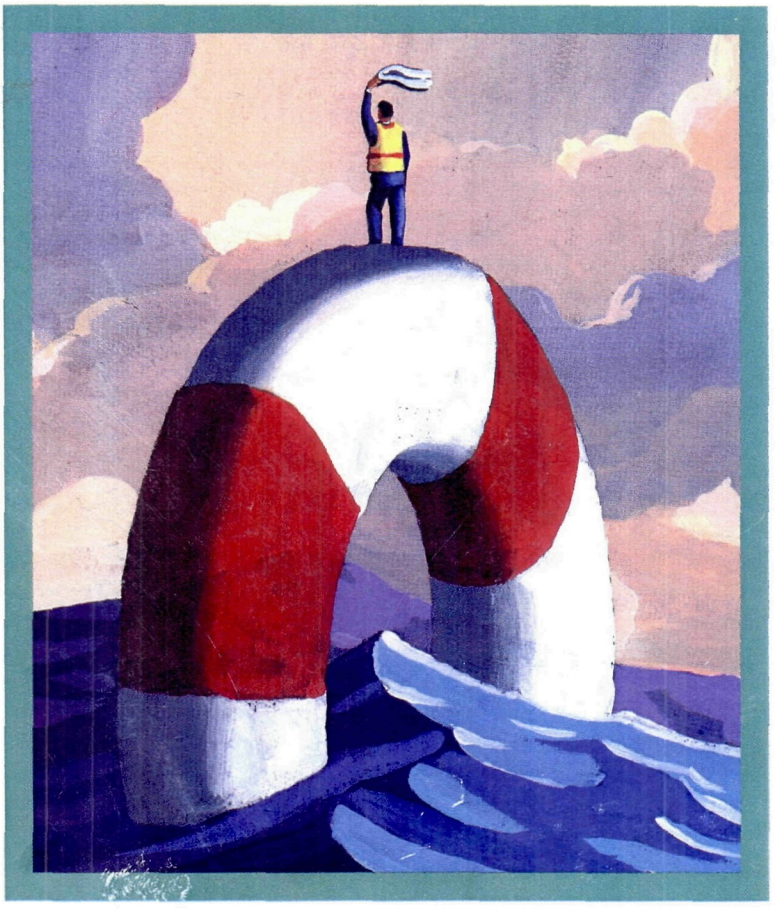
87-B Omega Drive
Newark, DE 19713
302-733-0980

2600 Glasgow Avenue
Newark, DE 19702
302-832-8894

Dover

830 Walker Road
Dover, DE 19901
302-730-8848

TRANSPORTATION AVAILABLE



We preserve livelihoods.

You can sink or swim depending on the insurance you choose. It's important to ensure that the things that matter most to you are protected. And Zutz has earned the endorsement of the state bar association. Why? More than half a century of experience insuring professionals just like you—offering coverage for virtually any specific need, including comprehensive life and health. Call us for a free consultation and brochure. We're here to make sure that you have the coverage you need to keep your livelihood safe.

The Zutz Group

INSURANCE

Since 1940

www.zutzgroup.com • Wilmington, DE: (302) 658-8000 or 1-800-441-9385 • London, England: 171-962-2003