STETSON UNIVERSITY COLLEGE OF LAW
26TH ANNUAL CONFERENCE ON LAW AND HIGHER EDUCATION
Clearwater Beach, Florida
February 19-23, 2005

OPENING PLENARY SESSION:

THE PATRIOT ACT, POST 9-11 POLITICS AND THE PROTECTION OF PRIVACY AND CIVIL RIGHTS IN THE UNIVERSITY COMMUNITY

PART I

WHAT YOU NEED TO KNOW ABOUT THE USA PATRIOT ACT—WHERE IT CAME FROM, WHAT'S IN IT, WHY IT'S BEEN CRITICIZED, AND WHAT MIGHT HAPPEN NEXT (LEGISLATIVELY)

Lawrence White
Chief Counsel
Pennsylvania Department of Education
Harrisburg, Pennsylvania

Note: The views expressed in this outline and the accompanying presentation are those of the author solely and should not be attributed to the author's place of employment or any other official or employee who works there.

INTRODUCTION: A BRIEF REFLECTION ON OUR STARTING POINT, FOLLOWED BY NOTES ON REFERENCES AND SOURCES

A. Sitting in Florida more than three years after the fact, we can't possibly conjure up the fears and emotions that roiled us collectively on September 11, 2001, when coordinated terrorist attacks ended the lives of more than 3,000 people in New York, Washington and Pennsylvania. We must nevertheless devote a few moments to the effort.

(1) *Images*. All the photographs in the PowerPoint presentation accompanying this outline are taken from the photo archive at www.september-11th.us, an idiosyncratic site with audio, video and text links to September-11-related material.[1]

[1] The site contains (at www.september-11th.us/Video-Tributes-Music-Flash.html) some astonishing and extremely graphic video clips of events at the World Trade Center that day. Other video, including coverage from the Pentagon and Pennsylvania, is available in an archive maintained on the CNN Web site at www.cnn.com/-SPECIALS/2001/trade.center/day.video.09.html.

[Footnote continued on next page.]

(2) *Text*.

- Just a month ago Times Books published 102 MINUTES: THE UNTOLD STORY OF THE FIGHT TO SURVIVE INSIDE THE TWIN TOWERS, a remarkable book by two *New York Times* reporters (Jim Dwyer and Kevin Flynn) that tells the story of the destruction of the World Trade Center from the horrifying, wrenching perspective of the people inside the towers on the morning of September 11.

  Nothing will bring back the memories of that day more vividly and painfully than this book.

  102 MINUTES shocks on two levels, the large-scale and the small-scale. It contains stunning numbers that lend perspective to the epic scale of death that day:

  - A total of 2,190 World Trade Center office workers and visitors killed (including 657 employees of a single company, the bond-trading firm Cantor Fitzgerald). Only 1,527 of the victims have been positively identified.[2]

  - 147 fatalities on the two aircraft that hit the towers.

  - 412 rescue workers killed.

  - About 600 building workers and visitors killed instantly by the impacts and explosions of the two airliners.

  - More than 1,500 World Trade Center office workers who survived the initial impacts killed when the buildings collapsed about an hour later.[3]

  As 102 MINUTES so tellingly relates, each death represented an unimaginable tragedy. The book uses transcribed radio transmissions, recorded phone messages, e-mails, and interviews with survivors and witnesses to chronicle what happened to hundreds of people inside the buildings. It will all come back to you as you read these accounts—the confusion, the lack of comprehension, the undirected anger, and the sense of incalculable, inexplicable, unnecessary loss.

Another source of extraordinary visual imagery is an exhibition titled "New York September 11" that was mounted at the New-York Historical Society just a few months after the events depicted. Selections from the exhibition can be viewed online at www.nyhistory.org/magnum911/index.html.

[2] That latter figure was reported by CNN on October 29, 2003. www.cnn.com/2003/US/Northeast/10/29/-wtc.deaths.

[3] In addition, 64 passengers on an American Airlines jetliner died when the plane was flown into the Pentagon that day, as did 124 people inside the Pentagon and 40 people on a United Airlines jetliner that crashed into an empty field near Shenksville in western Pennsylvania.

- From Andrew Sullivan, *Essay: Yes, America Has Changed*, TIME MAGAZINE, September 11, 2002, www.time.com/time/covers/1101020909/asullivan.html:

> We will forget. Researchers have long known that the memory of epochal events fades with time. Experts have a name for this phenomenon: flashbulb memory. As time passes, the chronology gets jumbled; we fumble on the details; we reimagine the past to make it more coherent, meaningful, bearable. We forget. We conflate. We confuse.
>
> But we know, of course, that this kind of memory is not the most important one. Some events solder themselves within our consciousness so intensely that they change forever the way we see the world. The details barely matter. The change itself matters. Events stop your life for a moment; your soul freezes while the rest of the world swivels around you to a new position. Part of you insists, This hasn't happened. Part of you demands, Move on. Most of you knows that neither is an option.
>
> And most of us know that there is no moving on from Sept. 11. It wasn't a random tragedy for which grief is a slow-acting salve. For whatever else Sept. 11 was, it was a declaration of war. The totalitarian force of radical fundamentalist Islam, like the forces of Nazism and communism that preceded it, has not disappeared. We briefly defanged it in its most important lair in Afghanistan, but even there it has not been extinguished. …
>
> [F]or all the return to superficial normality, Americans really have changed. The illusion of isolationism has been ripped apart. How can America opt out of the world when the world refuses to leave America alone? The illusion of appeasement has been destroyed. Do we really think that by coddling regimes like Iraq or Syria or Iran or Saudi Arabia, we will help defuse the evil that lurks in their societies? The illusion of American exceptionalism has been shattered. The whole dream of this continent—that it was a place where you could safely leave the old world and its resentments behind—was ended that day. A whole generation will grow up with this as its most formative experience—a whole younger generation that knows that there actually is a right and a wrong, and that neutrality is no longer an option. That generational power has only just begun to transform the culture. In decades' time, we will look back and see what a difference it made.

B. A bare seven weeks after September 11, Congress passed and President Bush signed into law a measure representing its first and best effort to endow the federal government with new powers to prevent future terrorist attacks. Like many legislative measures, this one represented a blend of ideas and approaches originating separately in the two houses of Congress. At the end of the day, proposed legislation introduced in the Senate as the

"Uniting and Strengthening America Act," or "USA Act," was combined with House-originated legislation called the "Provide Appropriate Tools Required to Intercept and Obstruct Terrorism Act," or "PATRIOT Act," and amalgamated into a bill with the tongue-twisting name "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001." In initial press reports and legislative communications, the bill was referred to by the unwieldy title "USA PATRIOT Act." With time, the popular name was shortened, first to the "PATRIOT Act" (with the capital letters paying homage to the longer name for which "PATRIOT" was an abbreviation), then, ultimately, the "Patriot Act." In this outline, for the sake of brevity, the law will be referred to by that short, lower-case moniker—the "Patriot Act."[4]

C. As major pieces of legislation go, the Patriot Act is medium-length—about 130 pages. It isn't easy reading. It uses the turgid, impenetrable language of legislative drafting, so that a typically elliptical section (in this case section 201, a provision titled "Authority to Intercept Wire, Oral, and Electronic Communications Relating to Terrorism") reads:

> Section 2516(1) of title 18, United States Code, is amended—
>
> (1) by redesignating paragraph (p), as so redesignated by section 434(2) of the Antiterrorism and Effective Death Penalty Act of 1996 (Public Law 104–132; 110 Stat. 1274), as paragraph (r); and
>
> (2) by inserting after paragraph (p), as so redesignated by section 201(3) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (division C of Public Law 104–208; 110 Stat. 3009–565), the following new paragraph:
>
> ''(q) any criminal violation of section 229 (relating to chemical weapons); or sections 2332, 2332a, 2332b, 2332d, 2339A, or 2339B of this title (relating to terrorism); or''.

As is often the case with abstruse legislation, the best way to penetrate the surface is not to read the act cover to cover, but instead to place yourself in the hands of a knowing secondary source. This outline borrows liberally from three excellent law review articles:

- Beryl A. Howell, *Seven Weeks: The Making of the USA PATRIOT Act*, in *The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy & The USA PATRIOT ACT*, 72 GEO. WASH. L REV. 1145 (2004). In 2001, when the Patriot Act was drafted, Howell served as General Counsel to the Senate Judiciary Committee and was one of the statute's principal architects. His law review article traces, on a day-by-day and even hour-by-hour

[4] Pub. L. No. 107-56, 115 Stat. 272 (2001). The text of the Patriot Act is available at several online locations. *E.g.*, http://news.findlaw.com/cnn/docs/terrorism/patriotact.pdf (a site maintained by Findlaw, a commercial legal resource company); http://thomas.loc.gov/cgi-bin/query/D?c107:4:./temp/~c107NsXudu:: (the Library of Congress); www.library.umass.edu/subject/patriotact (the library at the University of Massachusetts).

basis, the legislative machinations that shaped the Patriot Act as it made its way through Congress. The Howell article can legitimately lay claim to being the most detailed legislative history of the Patriot Act available from any non-governmental source.

- Patricia Mell, *Big Brother at the Door: Balancing National Security with Privacy Under the USA PATRIOT Act*, 80 DENV. U. L. REV. 375 (2002) (referred to in this outline as "*Mell*"). Professor Mell, a member of the faculty at Michigan State University Detroit College of Law, neatly summarizes—in about fifty pages of law review text—the Patriot Act's principal features. This is a good capsule introduction to the significant changes the Patriot Act made in preexisting surveillance and anti-terrorism law.

- David Lombard Harrison, *The USA PATRIOT Act: A New Way of Thinking, An Old Way of Reacting, Higher Education Responds*, 5 N.C. J. L. & TECH. 177 (2004). Harrison, a lawyer in the President's Office at the University of North Carolina, focuses on a handful of Patriot Act provisions—the ones that, in his view, impact higher education most directly.

I. PRE-PATRIOT-ACT SURVEILLANCE LAW

A. ***Introduction: A Very Quick Tutorial on "Intelligence" and Surveillance***. Throughout the Cold War and post-Cold-War periods in our nation's history, our national counterterrorism policy has been based on the preventive precept of *intelligence* (as in Central *Intelligence* Agency). Malevolent foreign powers and movements, so the tautology goes, operate through the actions of people. If the government knows in advance who and where those people are, what they're planning, what they're doing, what they're saying and writing—if it can gather and appropriately analyze *intelligence* about them—then it can prevent them from carrying out their plots.[5]

The government harvests intelligence by engaging in *surveillance*—what in a simpler time would have been called spying. Surveillance has been defined as the government's use of technical means to extract or create personal data—data on the movements and activities of individual persons—that can be analyzed for security purposes.[6] Here, then is our starting

[5] For a comprehensive introduction to the theory and vocabulary of American intelligence gathering, a good place to start is the "Intelligence Resource Program," a project (and Web site of the same name) maintained by the Federation of American Scientists (http://fas.org/irp). Particularly valuable is a Web page titled "Intelligence Programs and Systems" (http://fas.org/irp/program/index.html), which explains as lucidly as any non-classified site could how American intelligence agencies are organized and funded.

[6] This definition is adapted from Gary T. Marx, *What's New About the "New Surveillance"? Classifying for Change and Continuity*, 1 SURVEILLANCE & SOCIETY 9, 14 (2004).

[Footnote continued on next page.]

point for determining why Congress passed the Patriot Act in late 2001 and what it hoped to achieve—or, more accurately, prevent—by adopting the provisions in the Patriot Act.

(1) *Why, despite the enormity of the American intelligence-gathering machine, did September 11 happen?* One reason, according to the Congressionally-chartered 9/11 Commission, was because "[t]he U.S. government did not find a way of pooling intelligence and using it to guide the planning and assignment of responsibilities for joint operations involving entities as disparate as the CIA, the FBI, the State Department, the military, and the agencies involved in homeland security." In other words, there were structural problems with the way a multiplicity of overlapping agencies collected intelligence information, including inter-agency jealousies and turf battles, inadequate funding, and archaic bureaucratic structures. From the 9/11 Commission's final report:

> The intelligence community struggled throughout the 1990s and up to 9/11 to collect intelligence on and analyze the phenomenon of transnational terrorism.

The discrete intelligence disciplines define the different technologies by which intelligence is harvested:

(1) *Signals intelligence* (referred to in the intelligence community by the acronym "sigint") is the principal responsibility of the National Security Agency. Sigint involves the electronic interception of communications between members of a terrorist group or cell, using listening devices, de-encryption software, and other means.

(2) *Imagery intelligence* ("imint") is, as the name suggests, the analysis of images collected by satellites, manned aircraft and unmanned aerial vehicles. Imint is conducted by the National Geospacial-Intelligence Agency, the new name (as of 2004) for a consolidation of agencies including the old National Imagery and Mapping Agency and the defense Mapping Agency.

(3) *Human intelligence* ("humint") is the oldest and most venerable form of intelligence. Today it takes the form of human contacts—usually with foreign government officials and military officers—the substance of which are captured by listening devices or cameras or recorded in databases. The Central Intelligence Agency is the government's principal source of humint.

(4) *Secondary intelligence sources*, which include *open source intelligence* ("osint") (monitoring of newspapers, periodicals, pamphlets, books, radio, television, Internet websites, and other sources of non-classified information) and the emerging field of *measurement and signatures analysis* ("masint"), imprecisely defined as the use of computers to detect patterns in or otherwise to enhance raw intelligence gathered by sigint and imint sensors.

This typology is taken from U.S. Library of Congress, Congressional Research Service (Richard A. Best, Jr., author), INTELLIGENCE ISSUES FOR CONGRESS: A CRS ISSUES BRIEF FOR CONGRESS (updated December 9, 2004), available on the Web site of the Federation of American Scientists at www.fas.org/irp/crs/IB10012.pdf. An easier-to-digest typology is included in the report of the 9/11 Commission. *See* FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, Chapter 3 (*Counterterrorism Evolves*), July 22, 2004, www.9-11commission.gov/report/911Report.pdf.

> The combination of an overwhelming number of priorities, flat budgets, an outmoded structure, and bureaucratic rivalries resulted in an insufficient response to this new challenge.

FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, Executive Summary, July 22, 2004, www.9-11commission.gov/-report/911Report.pdf.

(2) *How, then, could another September 11 be prevented?* Among its many recommendations, the 9/11 Commission urged "a different way of organizing the government" to unify strategic intelligence operations, promote information sharing, improve Congressional oversight, and strengthen the government's intelligence-gathering capabilities:

> The men and women of the World War II generation rose to the challenges of the 1940s and 1950s. They restructured the government so that it could protect the country. That is now the job of the generation that experienced 9/11. Those attacks showed, emphatically, that ways of doing business rooted in a different era are just not good enough. Americans should not settle for incremental, ad hoc adjustments to a system designed generations ago for a world that no longer exists. …
>
> We recommend significant changes in the organization of the government. … The U.S. government cannot afford so much duplication of effort. There are not enough experienced experts to go around. The duplication also places extra demands on already hard-pressed single-source national technical intelligence collectors like the National Security Agency. … A "smart" government would integrate all sources of information to see the enemy as a whole. Integrated all-source analysis should also inform and shape strategies to collect more intelligence.

FINAL REPORT, *supra*, Chapter 13 (*How to Do It? A Different Way of Organizing the Government*), www.9-11commission.gov/report/911Report.pdf.

(3) *What are the obstacles?* There are three, all of which we explore in the next few sections of this outline.

(a) First, we Americans have always, always been innately suspicious about government surveillance.

(b) Second, that suspicion is institutionalized in American constitutional law—in the Fourth Amendment to the Constitution, which enshrines the principle that the government's ability to conduct surveillance should be procedurally and substantively restricted; in the Supreme Court case law construing Fourth Amendment protections; and in Congressional enactments defining the statutory law of surveillance.

(c) And third, surveillance is a nuanced, ever-evolving concept that poses different practical and legal issues depending on the context. Each form of intelligence—sigint, imint, humint, and so forth—is associated with a particular form of surveillance technology (listening devices, satellites, computers, and so forth) designed to enable government intelligence officials to collect and analyze information about the movements and activities of persons deemed threats to our domestic security. The public's willingness to sacrifice personal freedoms in the name of enhanced safety and security is highly context-specific. An interesting poll conducted by Michigan State University's Institute for Public Policy and Social Research just a few months after September 11 revealed the extraordinary range of public sentiment about surveillance methodology:

- By large majorities, citizens approved government surveillance of terrorist organizations.

- Citizens were split 50-50 in their support for national identification cards.

- But large majorities *disfavored* relaxation of warrant standards for telephone taps and e-mail surveillance, warrantless searches of the homes and offices of terrorist suspects, and the infiltration of non-violent domestic social action organizations.

"Following the September 11 attack, when asked in the abstract whether they think it is necessary to give up some rights for the sake of greater security, many Americans (45%) are willing to make trade-offs. Thus, in the abstract, American citizens are willing to sacrifice certain civil rights and personal freedoms for greater safety and security. In more specific terms, that willingness to sacrifice varies. When specific policies are considered, this willingness to concede civil rights depends on the right in question …." Institute for Public Policy and Social Research, *Policy Brief: Americans Protect Civil Liberties*, April, 2002, www.ippsr.msu.edu/Publications/-PBCivilLiberties.pdf.

B. ***The Constitutional and Statutory Framework***.

(1) *The Fourth Amendment*.

(a) Two centuries ago, before telephones and microphones and cameras, the standard form of government surveillance was the old-fashioned, knock-the-door-down *search* of physical premises and *seizure* of papers and other articles discovered by that means. American colonists hated searches and believed that English authorities routinely abused the common-law writs of general warrant and assistance to "search any place for any thing." *Mell* 381. To protect against abuse of the government's authority to conduct

unauthorized surveillance, the Fourth Amendment to the Constitution established "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures," one of the bedrock civil liberties established by the Bill of Rights.[7]

(b) How the Fourth Amendment works: The Fourth Amendment contains both an expression of substantive law (people possess "[t]he right … to be secure in their persons, houses, papers and effects") and a procedural standard (the government *may* conduct a search upon issuance of a warrant supported by probable cause and "particularly describing the place to be searched, and the persons or things to be seized"). Fourth Amendment jurisprudence, then, focuses on two questions:

- (The substantive-rights question:) Does government surveillance rise to the level of a Constitutionally protected *search*?

- (The procedural question:) If so, is the search *reasonable*? Is it either authorized by a warrant supported by probably cause or permissible as a narrow, judicially recognized exception to the warrant requirement?

(2) *Fourth Amendment Surveillance Jurisprudence*. "It is beyond question that the Fourth Amendment has been the subject of more litigation than any other provision in the Bill of Rights. Indeed, I would be willing to wager … that … lawyers and judges have spilled more words over the Fourth Amendment than all the rest of the Bill of Rights taken together." Wayne R. LaFave, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 1.1 (1st ed. 1978), *quoted in Mell* 382 n. 45. How are we to make sense of the enormous corpus of Fourth Amendment case law—or, more to the point, how are we to extract from the thousands of decided Supreme Court cases what we need to understand and appreciate Congress's intent when it enacted the surveillance provisions in the Patriot Act?

Although it took the Supreme Court a while to get to its resting point, the Court finally laid down a surprisingly useful and durable test for determining when government surveillance constitutes a "search" as that term is used in the Fourth Amendment—the so-called "reasonable expectation of privacy" test from *Katz v. United States*, 389 U.S. 347 (1967).

---

[7] U.S. Const. amend. IV. Although it's almost thirty years old, Professor Wayne LaFave's original treatise on the Fourth Amendment still contains one of the best histories of the colonial period leading up to the ratification of the Fourth Amendment at the end of the 18th century. *See* Wayne R. LaFave, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 1.1 (1st ed. 1978).

(a) *The problem*. The two-century-old language of the Fourth Amendment can't possibly mean what it literally says. On the one hand, a police officer strolling down the street would theoretically be engaging in surveillance—a "search," in constitutional terms—if he or she witnessed a crime in progress. The Fourth Amendment, read literally, suggests that the police officer couldn't chase down the suspected felon and make an arrest without first applying to a court for a warrant—not the result common sense suggests. On the other hand, our instincts tell us that the Fourth Amendment protects against the government's warrantless placement of a listening device on the telephone of a suspected mobster; yet the Fourth Amendment, read literally, protects only mobsters' "persons, houses, papers and effects"—nothing there about a workplace telephone. So what *does* the Fourth Amendment protect (and not protect)? That's the issue that has preoccupied courts for two centuries.

(b) *The early "trespass upon the property" test*. The Supreme Court propounded the first iteration of a general rule in *Olmstead v. United States*, 277 U.S. 438 (1928). *Olmstead* arose after federal law enforcement officials broke up a large bootlegging ring by means of information gathered by telephone taps. The taps, observed the Court, "were made without trespass upon any property of the defendants," but by connecting listening devices to trunk lines located in the basement of distant office buildings. 277 U.S. at 457. Adopting a highly mechanistic view of the Fourth Amendment, the Court ruled that the Amendment barred only searches of "material things"—searches effected through physical invasion of a person's real property, not searches of electronic transmissions dozens or even hundreds of miles from the person's home or physical presence. *Id.* at 458. Continued the Court:

> The [Fourth] Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses of offices of the defendants.
>
> By the invention of the telephone, fifty years ago, and its application for the purpose of extending communications, one can talk with another at a far distant place. The language of the [Fourth] Amendment can not be extended and expanded to include telephone wires reaching to the whole world from the defendant's house of office. The intervening wires are not part of his house of office any more than are the highways along which they are stretched. …
>
> [T]he Fourth Amendment [is not] violated as against a defendant unless there has been an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house "or curtilage" for the purpose of making a seizure.

> … We think, therefore, that the wire tapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment. [Id. at 465, 466.]

Over the next half-century, as government surveillance techniques grew in volume and sophistication, the Court continued to apply the "physical trespass" test from *Olmstead*, albeit with diminishing enthusiasm. *E.g.*, *Goldman v. United States*, 316 U.S. 129, 134 (1942) (federal agents did not conduct a search of a suspected criminal by placing an eavesdropping device against the interior wall of an office next to the suspect's because the surveillance did not involve "trespass or unlawful entry" of the suspect's office); *On Lee v. United States*, 343 U.S. 747 (1952) (no trespass—hence no search—when an informant wearing a hidden sound-recording wire was invited by the suspect into the latter's office); *Irvine v. California*, 347 U.S. 128 (1954) (the first Supreme Court decision to invalidate a conviction on the ground that evidence gathered through a surreptitious listening device was the fruit of unlawful physical trespass and hence constituted an impermissible search under the Fourth Amendment); *Silverman v. United States*, 365 U.S. 505 (1961) (the government, by hammering a so-called "spike mike" through a wall and into the office of a criminal suspect, violated the suspect's right to freedom from physical trespass under the Fourth Amendment).

Perhaps most significantly, in *Lopez v. United States*, 373 U.S. 427 (1963), the Court affirmed the criminal tax evasion conviction of a suspect secretly tape-recorded by an undercover Internal Revenue Service agent who invited himself into the suspect's office to solicit a bribe. The decision prompted an indignant dissent by Justice Brennan, who urged the Court to abandon the old "physical trespass" test in favor of a test based on both the "comprehensive right of privacy [and] individual freedom" underlying Fourth Amendment jurisprudence and a growing body of empirical evidence suggesting serious government abuse of electronic eavesdropping technology. 373 U.S. at 456, 467 (Brennan, J., dissenting).

(c) *Katz*, decided just a few years after *Lopez*, substituted a new "reasonable expectation of privacy" test for the old "trespass" test. In *Katz*, a criminal defendant was convicted of illegal gambling based in part on evidence obtained when agents placed a listening device on the outside of a public telephone booth. Lower courts upheld the conviction on the ground that the government had not conducted a "search" under the Fourth Amendment because "there was no physical entrance into the area occupied by [the petitioner]." 389 U.S. at 348. The Supreme Court reversed:

> [T]he "trespass" doctrine … can no longer be regarded as controlling. The Government's activities in electronically listening to and recording the

petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a "search and seizure" within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance. *Id*. at 353.

Katz stands for the proposition that the test for determining whether the government has conducted an unconstitutional search doesn't hinge on the place searched, but rather on the legitimate privacy expectations of the person subject to surveillance, regardless where that person is physically located. Katz and its linear ancestor, Justice Brennan's dissenting opinion in *Lopez*, also stand for the important proposition that Fourth Amendment jurisprudence must be sensitive to and informed by the need for "flexibility … to meet changing technologies." *International Society for Krishna Consciousness v. Lee*, 505 U.S. 672, 698 (1992). In other words, built into the flexible terminology of Fourth Amendment law—the *reasonable* nature of a search, the *legitimate* expectations of the subject of the search—is the notion that today's surveillance practices don't necessarily predetermine tomorrow's questions about the constitutionality of those practices. As surveillance technology evolves, so do judicial notions of propriety under the Fourth Amendment. And as context changes—as it indisputably did after September 11—so, arguably, do constitutional standards.[8]

(3) *Legislation on Surveillance Warrants.*

(a) "[B]y the 1960's it had become apparent that … the privacy rights of thousands of Americans had been unlawfully violated." Michael Goldsmith, *Criminal Law: The Supreme Court and Title III: Rewriting the Law of Electronic Surveillance*, 74 J. CRIM. L. & CRIMINOLOGY 1, 34 (1983). In 1965, in response to growing expressions of concern over the increase in crime and the spreading influence of organized racketeering, Lyndon Johnson created the President's Commission on Law Enforcement and Administration of Justice, popularly known as the President's Crime Commission. The Commission's landmark 1967 report is widely regarded as the first systematic examination of government electronic surveillance practices. "The present status of the law with respect to wiretapping and bugging," concluded the report, "is intolerable." The report recommended the adoption of comprehensive legislation authorizing electronic surveillance under a system of strict, court-supervised controls. President's Crime Commission, THE CHALLENGE OF CRIME IN A FREE SOCIETY 203 (1967). *See* G. Robert Blakey &

[8] For comprehensive treatments of the Supreme Court's surveillance jurisprudence, *see* Michael Goldsmith, *Criminal Law: The Supreme Court and Title III: Rewriting the Law of Electronic Surveillance*, 74 J. CRIM. L. & CRIMINOLOGY 1, 7-32 (1983); *Mell* 382-89.

Brian Gettings, *Racketeer Influenced and Corrupt Organizations (RICO): Basic Concepts—Criminal and Civil Remedies*, 53 TEMPLE L.Q. 1009, 1014-15 (1980).

(b) *Title III and domestic surveillance*. In June, 1968, Congress passed the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. §§ 2510 *et seq*. It was a grim time in the history of the country—three months after the assassination of Dr. Martin Luther King, days after the assassination of presidential candidate Robert F. Kennedy, and in the middle of an emotional presidential campaign featuring Republican nominee Richard Nixon's memorable pledge to be "tough on crime." Title III of the Act "was the culmination of a forty[-]year debate concerning the utility and constitutionality of electronic surveillance." At its heart is a "conscious compromise forged by Congress between competing privacy and law enforcement concerns." Title III authorizes the use of the most common forms of electronic surveillance—"wiretaps" and "bugs"[9]—subject, however, to prior judicial approval and compliance with stringent statutory requirements. Michael Goldsmith, *Criminal Law: The Supreme Court and Title III: Rewriting the Law of Electronic Surveillance*, 74 J. CRIM. L. & CRIMINOLOGY 1, 3-4 (1983).

- Title III by its terms does not apply to foreign intelligence surveillance—the province of the Foreign Intelligence Surveillance Act of 1978 (see the next section of this outline.)

- "Title III is restrictive in tone; all electronic surveillance is prohibited, except as specifically provided therein. … Title III takes the form of a series of limitations and prohibitions on lawful eavesdropping; the 'do's' are largely the residue of multitudinous 'don'ts'." Goldsmith, *supra*, 74 J. CRIM. L. & CRIMINOLOGY at 39-40 (internal quotation omitted).

- Under Title III, a warrant to conduct electronic surveillance will not issue unless four prerequisites are satisfied:

  - *Jurisdictional requirements*. The warrant must be signed by an authorized executive official (the Attorney General or designee) and filed with a court of competent jurisdiction;

[9] These terms are placed in quotation marks because they are statutorily defined in Title III. *See* 18 U.S.C. § 2510(1), (2). The definitions were amended in several pertinent respects by the Patriot Act. Pub. L. No. 107-56, § 224, 18 U.S.C. § 2510 note.

- *Documentary requirements.* The application for a warrant must be submitted under oath; must describe with particularity the subject of surveillance and the nature of surveillance to be used; and must recite facts sufficient to establish probable cause to believe that criminal activity has occurred or will occur.

- *Requirements for the execution of a warrant*. Surveillance can be conducted only by properly authorized personnel and in accordance with statutory recordation and chain-of-custody rules.

- *Ongoing judicial supervision*. Title III allows the supervising judge to require submission of periodic reports or use other mechanisms to ensure compliance with all statutory requirements. 18 U.S.C. § 2518.

All these prerequisites are designed to ensure that warrants "meet the test of the Constitution that electronic surveillance techniques be used only under the most precise and discriminate circumstances…." [10]

Quick Title III summary: For the better part of forty years Title III has been—and remains today—the preeminent expression of Congressional policy on domestic electronic surveillance. While critics complain that Title III tilts the playing field in favor of the government,[11] the statute contains important safeguards to ensure that surveillance is conducted under judicial supervision, in accordance with strict procedural requirements, and only when demonstrably necessary.

(c) *FISA and national security surveillance*. Unsurprisingly, Americans have always been more tolerant of surveillance when it's directed at foreigners,[12]

---

[10] The language in quotation marks is from the Senate Committee Report accompanying the legislation ultimately enacted as the Omnibus Crime Control and Safe Streets Act of 1968. S. Rep. No. 1097, 90th Cong., 2d Sess. 66, *reprinted in* 1968 U.S. CODE CONG. & AD. NEWS 2112, 2157-58. It is quoted in Goldsmith, *supra*, 74 J. CRIM. L. & CRIMINOLOGY at 42.

[11] For discussion of the criticisms leveled at Title III, *see* Goldsmith, *supra*, 74 J. CRIM. L. & CRIMINOLOGY at 44-56. The principal grounds of attack include the following:

- "[T]oo much electronic surveillance [is] not subject to the warrant requirement";
- The statute permits "judge shopping"—the identification of surveillance "hawks" to whom applications for warrants can be repeatedly directed.

[12] *See generally* Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. PA. L. REV. 793, 795-805 (1989) (cited on succeeding pages of this outline as ("A.R. Cinquegrana, *The Walls*"). As late as the 1930s the U.S. Attorney General formally took the position that foreign surveillance, "while perhaps raising ethical issues, was not unlawful." *Id.* at 796. During World War II President Roosevelt ordered his Attorney General to deploy "listening devices" when needed for national security purposes, a practice continued in peacetime by President Truman. It was not until the

[Footnote continued on next page.]

and an entirely different set of statutory rules come into play when the government wishes to conduct surveillance, not for domestic crime-fighting purposes, but for the purpose of foreign intelligence gathering.

As already stated on page 13 of this outline, Title III of the Omnibus Crime Control and Safe Streets Act contains a carve-out for foreign intelligence surveillance. Even before Congress enacted Title III, the Supreme Court in a short but famous footnote in its *Katz* decision expressly reserved judgment on the question whether the government needed a warrant for surveillance justified on national security grounds.[13] Four years after passage of Title III, the Court made the same point more explicitly in *United States v. United States District Court*, 407 U.S. 297 (1972). In that case, the defendant in a criminal prosecution arising from the bombing of a CIA field office in Ann Arbor, Michigan, during an anti-war protest sought to suppress transcripts of government wiretaps obtained without first securing a warrant under Title III. Attorney General John Mitchell represented to the Court that no warrant was required when surveillance was determined to be "necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government." 407 U.S. at 301. The Court drew a careful distinction between surveillance of *domestic* organizations and surveillance of "the activities of foreign powers," *id.* at 308, and held that, while the former required probable cause and a warrant, the latter did not:

> We emphasize, before concluding this opinion, the scope of our decision. As stated at the outset, this case involves only the domestic

---

presidency of Lyndon Johnson and the establishment of the President's Crime Commission that national security wiretaps were subjected to judicial approval. Between 1940 and the mid-1960s, the Justice Department performed 7,000 warrantless wiretaps and more than 2,000 telephone taps in the name of protecting national security. *Id.* at 798-99.

Courts too recognize doctrinal differences between domestic and foreign surveillance. In a series of cases decided in the 1970s, appellate courts held that electronic surveillance of foreign powers and their agents operating in the United States was permissible without a warrant under a "recognized exception" to the warrant requirement in the Fourth Amendment. United States v. Buck, 548 F. 2d 871, 875-76 (9th Cir.), *cert. denied*, 434 U.S. 890 (1977). *Accord*, United States v. Brown, 484 F. 2d 418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974); United States v. Butenko 494 F. 2d 593 (3d Cir.) (en banc), *cert. denied*, 419 U.S. 881 (1974).

[13] "Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case." Katz v. United States, 389 U.S. 347, 358 n. 23 (1968). In a concurring opinion that was barely longer than that footnote, Justice White reiterated the point: "I note the Court's acknowledgment that there are circumstances in which it is reasonable to search without a warrant. In this connection, in footnote 23 the Court points out that today's decision does not reach national security cases. … We should not require the warrant procedure and the magistrate's judgment if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable." *Id.* at 363 (White, J., concurring).

> aspects of national security. We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents. … [W]arrantless surveillance, though impermissible in domestic security cases, may be constitutional where foreign powers are involved…. [*Id*. at 321-22, 322 n. 20.]

In the mid-1970s, the Watergate scandal and widespread unease over the extent to which the Nixon Administration had abused the national security apparatus to assemble intelligence on his political enemies[14] prompted the Democratically controlled Senate to establish a select committee on intelligence abuses. Senator Frank Church chaired the committee, which held widely publicized hearings during the summer of 1975. The "Church Committee," as it was colloquially known, issued an influential report the next year that called, among other measures, for the passage of legislation imposing statutory discipline on the process for preauthorizing electronic surveillance for foreign intelligence purposes.[15]

That legislation was the Foreign Intelligence Surveillance Act, signed into law by President Carter in 1978.[16] FISA establishes a separate statutory regime governing the standards and procedures for the authorization of foreign intelligence surveillance. The salient features of that regime:

- *A unique forum*. FISA created a special court—the Foreign Intelligence Surveillance Court, or "FISC"—to hear applications for orders authorizing foreign intelligence surveillance. FISC consisted of seven federal district judges appointed by the Chief Justice of the United States. Applications are heard *in camera*—in other words, in secret without notice to the subject of surveillance—under conditions of secrecy and physical security designed to protect sensitive national security information. 50 U.S.C. §

---

[14] *See generally* A.R. Cinquegrana, *The Walls* 806.

[15] *Book II—Intelligence Activities and the Rights of Americans: Final Report of the Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities*, S. Rep. No. 755, 94th Cong., 2d Sess. (1976). The Church Committee Report is available online on a Web site maintained by a nonprofit organization, the Assassination Archives and Research Center, and can be accessed from a link on the Michigan State University Libraries Web site at http://er.lib.msu.edu/item.cfm?item=043387.

[16] Pub. L. No. 95-511, 92 Stat. 1783, *codified at* 50 U.S.C. §§1801 *et seq*. and 18 U.S.C. §§ 2518-19.

FISA is a complex piece of legislation, and a detailed consideration of its many convoluted provisions is beyond the scope of this outline. For those interested in relatively concise introductory treatments, *see* A.R. Cinquegrana, *The Walls*; Sharon H. Rackow, *How the USA PATRIOT Act Will Permit Governmental Infringement Upon the Privacy of Americans in the Name of "Intelligence" Investigations*, 150 U. PA. L. REV. 1651, 1661-74 (2002). (This article is cited in succeeding pages as "Rackow, *Infringement*".)

1803(c). Government appeals are taken to a three-judge panel whose members are also appointed by the Chief Justice.[17]

- *Circumscribed purpose*. Perhaps no provision in FISA was more crucial than the "purpose" clause, which provided originally that a judge could issue a court order permitting foreign intelligence surveillance only when "the purpose of the surveillance is to obtain foreign intelligence information." 50 U.S.C. § 1804(a)(7)(B) (1994).[18] In other words, a FISA order was available *only* for the purpose of facilitating foreign intelligence surveillance; if intelligence were sought for a secondary purpose—for example, fighting domestic crime—then Title III (with its rigorous warrant requirement) was the only avenue for obtaining an order and the more relaxed standards in FISA were unavailable.

- *A more relaxed standard for probable cause*. Title III contained the traditional probable cause standard in criminal cases: the government was obliged to adduce facts sufficient to give an impartial judge or magistrate "probable cause for belief that an individual is committing, has committed, or is about to commit a [criminal] offense." 18 U.S.C. § 2518(3)(a). This is a "high threshold of proof." Rackow, *Infringement*, 150 U. PA. L. REV. at 1681. But FISA uses a more relaxed standard: the authorizing judge must find probable cause—not that a crime has been or is about to be committed—but that the target of surveillance is a foreign power or foreign agent, and that the place at which electronic surveillance is directed is being or will be used by a foreign power or an agent of a

[17] That court's appellate docket is extremely light, if it exists at all. In the first ten years following passage of FISA, the government applied for 4,278 surveillance orders; FISC *granted* orders in all 4,278 cases—in other words, the government had no refusals to appeal. A.R. Cinquegrana, *The Walls* 814.

Over the past five years, FISC granted orders in 5,774 of 5,778 cases. The government elected not to appeal the four cases in which FISC denied its applications.

Calendar Year	*Applications Filed*	*Applications Granted*	*Applications Denied*	*Appeals*
1999	886	886	0	0
2000	1,005	1,005	0	0
2001	932	932	0	0
2002	1,228	1,228	0	0
2003	1,727	1,723	4	0
TOTALS:	5,778	5,774	4	0

Figures compiled from U.S. Dep't of Justice, *Foreign Intelligence Surveillance Act Annual Reports*, available online at www.justice.gov/oipr/readingroom/oipr_records.htm.

[18] As we'll see on pages 21-22 of this outline, the "purpose" clause was significantly amended by the Patriot Act. The text quoted on this page of the outline represents the pre-amended version.

foreign power. Under FISA, "the role of the judge … is minimal" and results in "less stringent [judicial] review." *Id.* Not surprisingly, courts consider Attorney General applications for FISA orders to be "presumptively valid" and rarely accord them more than cursory examination. Sherri J. Conrad, *Executive Order 12,333: "Unleashing" the CIA Violates the Leash Law*, 70 CORNELL L. REV. 968, 979 (1985).

Quick FISA summary: FISA represented a distinctive compromise. Until its enactment in 1978, the Fourth Amendment (arguably) imposed no fetters on the government's ability to conduct foreign intelligence surveillance. FISA created a system of judicial preapproval, but one that was decidedly more flexible—and more deferential to the government—than what existed in the domestic crime-fighting context. To make sure that flexibility wasn't abused, FISA clearly and unambiguously applied only to surveillance undertaken for foreign intelligence purposes—a delimiting boundary that quickly eroded after September 11.

II. THE CHANGES EFFECTED BY THE PATRIOT ACT

A. *Overview of the Patriot Act*

(1) Attached as an appendix to this outline is the Patriot Act's table of contents. The Act is divided into ten freestanding divisions or "titles," the most important of which are the following:

- Title II, "Enhanced Surveillance Procedures"—amendments to Title III, FISA, and other surveillance laws;

- Title III, "International Money Laundering Abatement and Antiterrorist Financing Act of 2001"—a lengthy new law addressing money-laundering practices by foreign terrorist organizations;

- Title IV, "Protecting the Border"—immigration reform measures, including provisions for tracking the whereabouts of foreigners holding student visas;

- Title V, "Removing Obstacles to Investigating Terrorism"—a miscellany of provisions important (for our purposes) because of the amendment it makes to the Family Educational Rights and Privacy Act of 1974; and

- Title VIII, "Strengthening the Criminal Laws Against Terrorism"—definitions of new terrorism-related federal crimes.

In the next two sections of the outline we'll briefly describe the most important provisions from these titles in the Patriot Act.

B. ***What the Patriot Act Did to Pre-Existing Surveillance Law*** [19]

(1) *What it did to Title III*:

- *Grand jury secrecy*. Section 203 of the Patriot Act significantly modifies one of the most venerable rules in the Federal Rules of Criminal Procedure: Rule 6, which prohibits the disclosure of grand jury testimony. As Rule 6 is amended by the Patriot Act, the subject matter of grand jury testimony can now be disclosed, without a subpoena, "to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties," so long as the testimony involves "foreign intelligence or counterintelligence … or foreign intelligence information."

- *E-mail and Internet surfing*. Section 216 is a controversial provision that broadens the definitions of certain forms of electronic surveillance—pen registers and trap-and-tape devices—for the purpose of extending permissible surveillance to include suspects' utilization of computers to surf the Net and send and receive e-mail messages.

  This section "has the potential to be one of the broadest changes to prior law, and may have the most long-term effect of [the Patriot Act], given the increasing importance of the Internet for communications. It makes three significant changes to prior law. First, the amendments … clarify that the pen/trap statutes apply to Internet and other computer network traffic, provided that the devices do not include the contents of communications. … This provides clear authority to use software instead of just physical mechanisms. Second, the section allows courts to issue orders that are valid anywhere in the United States, not just their own jurisdiction. This recognizes the deregulation of communications providers and

[19] The following pages of the outline treat only a handful of the many changes in substantive law made by the Patriot Act. I have focused on the changes most pertinent to the higher education community. For those desiring a more comprehensive, although not necessary objective, treatment of the Act, here are some online resources:

- Electronic Privacy Information Center, *The USA Patriot Act*, www.epic.org/privacy/terrorism/usa-patriot.
- U.S. Library of Congress, Congressional Research Service, THE USA PATRIOT ACT: A LEGAL ANALYSIS, available on the Web site of the Federation of American Scientists at www.fas.org/irp/crs/-RL31377.pdf (long but very comprehensive). The Congressional Research Service also prepared a short summary entitled, appropriately enough, THE USA PATRIOT ACT: A SKETCH. It's online at www.fas.org/irp/crs/RS21203.pdf.
- The U.S. Department of Justice's official Patriot Act Web site, www.lifeandliberty.gov.

avoids the necessity to seek multiple supporting orders. Thus, an ISP may be presented with an order from a court outside its own state and which does not name the ISP specifically. … Third, if the ISP is unable to gather the information requested by its own capabilities and the FBI installs its [own] … device, it must then make a report to the court concerning the installation, configuration, and information collected." David Lombard Harrison, *The USA PATRIOT Act: A New Way of Thinking, An Old Way of Reacting, Higher Education Responds*, 5 N.C. J. L. & TECH. 177, 193-94 (2004).

(2) *What it did to FISA*:

- *Roving wiretaps*. Until the mid-1980s, government applications for wiretapping warrants under Title III were required to specify the actual telephone the government wanted to tap. In the mid-1980s, Congress amended Title III to permit "roving" taps—taps of any phone a particular suspect used, thereby "allowing agents the ability to target their surveillance on an individual, rather than a particular telephone." Rackow, *Infringement*, 150 U. PA. L. REV. at 1683. Sensitive to the fact that roving taps opened the way to potential abuse, Congress added some restrictions "as a means of protecting an innocent conversant from unnecessary invasion of privacy," *id.*, the most significant of which was *geographical*: a judge could authorize a roving tap only upon a showing that the suspect was using a second phone line "reasonably proximate" to the line identified in the original warrant application.

  Section 206 of the Patriot Act authorizes roving wiretaps under FISA—in other words, taps not of domestic criminal suspects under Title III but suspected foreign agents under FISA. "Advances in technology clearly justify modifying FISA to allow intelligence surveillance to meet the growing use of cellular phones, pagers, and e-mail, all portable means of communication that may have the effect of thwarting surveillance." *Id*. at 1684. But for reasons not clearly explained in the legislative history of the Patriot Act, the new roving wiretap provision in FISA omits the "reasonably proximate" limitation in Title III. As one commentator noted:

  > [P]ursuant to FISA authority, an agent may now wiretap a telephone even if it is unclear whether the target is actually using the telephone, or is reasonably close to it. An agent can wiretap and listen to a phone line in an innocent individual's home for the entire day, if the agent had information that the target was expected to visit that person at some point during a given twenty-four hour period. … This means that the private conversations of the individuals who live in this particular home, as well as the conversations of all people they speak with on the telephone over the course of that day, will be intercepted by the government without sufficient justification. If section 206 contained a protection similar to the "reasonably proximate" provision [that]

> Title III affords, the government would not be able to listen to every conversation held on this phone line throughout the day, but rather only those taking place when the target is actually in that person's home. Considering the number of telephones or modes of communication a given target could use during the course of a ninety-day surveillance, it becomes clear just how many private conversations could be listened to for "intelligence" purposes.

Id. at 1684-85.

Bottom line: Section 206 of the Patriot Act sensibly enables the government to engage in national security surveillance of suspects who use modern modes of communication (cellular phones, wireless PDAs, computers), but omits safeguards designed to prevent overbroad surveillance of third parties.[20]

- *Extension to domestic terrorism investigations.* The pre-Patriot-Act version of FISA drew an important line of demarcation between investigations targeting foreign powers (covered by FISA) and investigations targeting suspected domestic criminals (covered by Title III). The distinction was crucial because of the relaxed probable cause standard under FISA. It was easier, in other words, to obtain a court order approving FISA surveillance, but that advantage was offset by the limited circumstances under which the government could apply for a FISA order: only if "*the purpose* of the surveillance" was to obtain foreign intelligence. (See page 17 of this outline.)

  One of the most controversial provisions in the Patriot Act is section 218, a short, seemingly innocuous provision that reads in its entirety as follows:

  > Sections 104(a)(7)(B) and section 303(a)(7)(B) (50 U.S.C. §§ 1804(a)(7)(B) and 1823(a)(7)(B)) of the Foreign Intelligence Surveillance Act of 1978 are each amended by striking "the purpose" and inserting "a significant purpose".

  No longer is foreign intelligence the one and only purpose for which the government may seek an easier-to-obtain surveillance order under FISA. Now foreign intelligence need be only one of two or more purposes. Without satisfying the probable cause standard in Title III, the government can now obtain a *FISA surveillance order* to investigate suspected *domestic terrorism*—a significant

[20] For a more detailed critique, *see* Electronic Privacy Information Center, *Foreign Intelligence Surveillance Act (FISA*), www.epic.org/privacy/terrorism/fisa.

change in existing search-and-seizure law, and one that has drawn the wrath of civil libertarians.[21]

- *Business records (including library records).* Under the pre-Patriot-Act version of FISA, the government had the right to demand the production of "business records" as part of a foreign intelligence investigation, but the term "business records" was narrowly defined to include only *certain* records maintained by *certain* businesses—telephone records, rental car receipts, bills of lading from warehouses, and a few others. But section 215 of the Patriot Act eliminates the references to particular categories of records and substitutes the following open-ended language: "any tangible things (including books, records, papers, documents, and other items)."

  Among the most vocal critics of section 215 is the library community, which has repeatedly expressed its fear that the government will use this provision to compel the production of sensitive patron records.[22] The higher education community too has voiced concern over the possibility that a wide range of research materials could conceivably come within the reach of the "business records" provision in FISA as amended by the Patriot Act.[23]

C. ***What Else the Patriot Act Did***

- *FERPA.* The Family Educational Rights and Privacy Act of 1974—"FERPA" or the "Buckley Amendment" in the parlance of the higher education community—is the principal federal statute protecting the confidentiality of education records.[24] Animated in part by the fact that Mohamed Atta and Marwan al-Shehhi, two of

---

[21] *See* sources cited in Michael T. McCarthy, *Recent Development: USA Patriot Act*, 39 HARV. J. ON LEGISLATION 435, 444 nn. 63-66 & accompanying text (2002). (This article is cited in the next few pages of this outline as "McCarthy, *Recent Development*".)

[22] *See* American Library Association, *Guidelines for Librarians on the U.S.A. Patriot Act*, January 19, 2002, www.ala.org/ala/washoff/WOissues/civilliberties/theusapatriotact/patstep.pdf; U.S. Library of Congress, Congressional Research Service, LIBRARIES AND THE USA PATRIOT ACT, February 26, 2003, www.ala.org/ala/-washoff/WOissues/civilliberties/theusapatriotact/CRS215LibrariesAnalysis.pdf.

[23] David Lombard Harrison, *Higher Education Issues After The USA Patriot Act*, an undated paper prepared for the Legal Reference Service of the National Association of College and University Attorneys and available online at www.nacua.org/documents/PatriotAct_Outline.pdf.

[24] 20 U.S.C. § 1232g. *See* American Association of Collegiate Registrars and Admissions Officers, *Practical Online Guide to the Family Educational Rights & Privacy Act*, www.aacrao.org/ferpa_guide/enhanced/main_-frameset.html; National Academic Advising Association, *FERPA: Basic Guidelines for Faculty and Staff—A Simple Step-by-Step Approach For Compliance* (William R. Van Dusen, Jr., 2004), www.nacada.ksu.edu/Resources/-FERPA-Overview.htm.

the September 11 hijackers, entered the country on student visas and received some of their training at a Florida flight school,[25] Congress amended FERPA in the Patriot Act to make it easier for government agents to obtain education records on suspected terrorists.

Section 507 of the Patriot Act amends FERPA in two respects:

First, it authorizes the Attorney General to seek an *ex parte* order compelling a college or university to turn over educational records pertaining to any individual suspected of "domestic or international terrorism." To obtain such an order, the Attorney General is *not* required to show probable cause; instead, all that's required is a showing of "specific and articulable facts giving reason to believe that the education records are likely to contain information" relevant to the investigation. "[T]he reasonable suspicion standard … [is] a much lower standard than the probable cause standard. Where probable cause requires law enforcement officials to know what they are looking for before they look for it, reasonable suspicion does not. As a result, using reasonable suspicion has traditionally been used as justification for only minor privacy invasions, such as when police officers pat down an individual exhibiting unusual or suspicious behavior. Poring over a student's education records is not such a minor intrusion." American Civil Liberties Union of Ohio, *Impact of the USA PATRIOT Act on FERPA* (August, 2002), www.acluohio.org/publications/ferpa.pdf.

Second, one of FERPA's signature requirements is that a college or university maintain a written log of "all individuals …, *agencies*, or *organizations* which have requested or obtained access to a student's education records …." 20 U.S.C. § 1232g(b)(4) (emphasis added). The Patriot Act does away with this notice obligation in two respects: first, by amending FERPA to eliminate the logkeeping requirement for terrorism-related productions; and, second, by allowing the government to obtain orders *ex parte* without providing traditional notice to the subject of the record.

It is no exaggeration to say that the higher education community is anxious about government requests for education records under section 507 of the Patriot Act. In the months following September 11, more than 200 colleges and universities produced records in response to *ex parte* orders obtained by the Federal Bureau of Investigation, the Immigration and Naturalization Service, and other federal law

[25] David Johnston, *6 Months Late, I.N.S. Notifies Flight School of Hijackers' Visas*, N. Y. TIMES, March 13, 2002, available online at http://propagandamatrix.com/6_months_late_ins_notifies_flight_school.html.

enforcement agencies,[26] prompting some national higher education organizations to express apprehension about the dilution of FERPA protections.[27]

- *Money laundering*. Near the end of Congressional consideration, another bill that was on a separate legislative track—the International Money Laundering and Abatement and Anti-Terrorist Financing Act of 2001—was plopped into the Patriot Act and became the longest title in the whole bill. The money laundering provisions consume almost half the total number of pages in the Act.

  The purpose of these monstrously complex provisions is to disrupt terrorist financial networks by requiring banks and other financial institutions to monitor account activity and report suspicious transactions. The money laundering provisions also expand the authority of the Secretary of the Treasury to regulate the often complex relationships between American and foreign banks, including the authority to prohibit U.S. financial institutions from maintaining correspondent accounts for foreign shell banks; create several new federal money laundering crimes; and authorize new forfeiture and confiscation procedures.[28]

  In one recent law review article, a financial institutions specialist warned that the money laundering provisions in the Patriot Act could affect the operations of college and university business officers, bursars offices and credit unions and suggested that "[a] review of financial functions throughout the university should be undertaken … to ascertain which of the categories apply to individual universities and which sections of the USA PATRIOT Act [money laundering provisions] will apply to activities at any particular institution." Cynthia J. Larose, *International Money Laundering Abatement and Anti-Terrorism Financing Act of 2001*, 30 J. COL. & UNIV. L. 417, 419 (2004).

- *New definitions of "terrorist organizations" and "domestic terrorism."* Under the Immigration and Naturalization Act, a "foreign terrorist organization" is an organization identified by name on a short list maintained for that purpose by the Secretary of State. U.S. Dep't of State, Office of Counterterrorism, *Fact Sheet* (December 29, 2004), http://www.state.gov/s/ct/rls/fs/2004/37191.htm. Section 411 of the Patriot Act "expands the definition to include any group that engages in

---

[26] American Civil Liberties Union, *How the USA-Patriot Act Puts Student Privacy at Risk* (2002), www.asata.org/resources/articles/civil_rights/ACLU_student_privacy.pdf.

[27] *See, e.g.*, National Association of Student Financial Aid Administrators, *USA PATRIOT ACT Results in Amendments to FERPA; NASFAA Training Materials Updated*, June 12, 2002, posted online at www.nasfaa.org/-publications/2002/ctferpaupdate061202.html.

[28] *See generally* U.S. Library of Congress, Congressional Research Service, THE USA PATRIOT ACT: A LEGAL SKETCH 3-5, available on the Web site of the Federation of American Scientists at www.fas.org/irp/-crs/RS21203.pdf; McCarthy, *Recent Development*, 39 HARV. J. ON LEGISLATION at 448.

violence or destruction of property"—an expansion so broad that one commentator has wondered aloud whether it "infringes on association rights of non-citizens." McCarthy, *Recent Development*, 39 HARV. J. ON LEGISLATION at 450.

Section 802 of the Patriot Act adds to the federal criminal code a new crime—"domestic terrorism." It's very broadly defined to encompass (and I'm eliding here for the sake of grammatical clarity) "acts dangerous to human life … [that] appear to be intended to intimidate or coerce a civilian population." As one commentator has perceptively noted: "[M]any acts of political dissent and activism [could] now … be characterized as 'domestic terrorism.' Such a broad definition for a wide range of underlying crimes greatly increases the number of activities that likely will fall within the USA PATRIOT Act's scope. As the definition of 'domestic terrorism' stands, it encompasses activities ranging from those of anti-abortion activists who use violence against women entering Planned Parenthood clinics, to World Trade Organization protesters who throw rocks through the windows of merchants and politicians who publicly support the WTO. … [Congress] may be handing a future administration tools to investigate pro-life or gun rights organizations on the grounds that fringe members of their movements advocate violence. It is an unfortunate reality that almost every political movement today, from gun rights to environmentalism, has a violent fringe." Rackow, *Infringement*, 150 U. PA. L. REV. at 1688-89.

- *Student visa monitoring*. In 1996, as part of the Illegal Immigration Reform and Immigrant Responsibility Act, Pub. L. No. 104-208, 8 U.S.C. § 1372, Congress directed the agency then known as the Immigration and Naturalization Service (now known as United States Citizenship and Immigration Services, part of the Department of Homeland Security) to develop and operate a program to collect current information from universities and exchange programs on nonimmigrant foreign students studying in the United States. Section 416 of the Patriot Act calls for full implementation of the computerized tracking system known as the Student and Exchange Visitor Information System, or "SEVIS" for short, and appropriates $36 million to assist in the process. In one of the Act's most obvious references to September 11, Section 416 also expands the SEVIS program to cover "air flight school[s], language training school[s], [and] vocational schools," which of course were not covered under the 1996 legislation.
  SEVIS proved to be user-unfriendly, and the INS delayed the go-live date several times. Michael Arnone, *Problems Continue to Plague Database that Tracks Foreign Students*, CHRON. OF HIGHER ED., April 4, 2003, page A26.[29]

[29] As one of my co-panelists Sylvia Kless wrote in an article that appeared in the CHRONICLE OF HIGHER EDUCATION just a few months ago:

[Footnote continued on next page.]

- *Biohazardous agents*. Section 817 of the Patriot Act expands preexisting restrictions on the possession and use of biological agents and toxins. Section 817 adds to the federal criminal code a new offense making it a felony to "possess[ ] any biological agent, toxin, or delivery system of a type or in a quantity that, under the circumstances, is not reasonably justified by a prophylactic, protective, *bona fide research*, or other peaceful purpose [emphasis added]." (The language in italics was added after strenuous lobbying by the higher education community. *See* American Council on Education, *Continued Commitment to Secure Handling of Biohazardous Materials*, November 1, 2001, www.acenet.edu/washington/-anti_terror/2001/11november/biohazard.1101.cfm.) Section 817 also prohibits the shipment or possession of biohazardous material by "restricted persons," a term defined statutorily to include felons, fugitives, drug abusers, illegal immigrants, and persons with dishonorable military discharges. Many universities now require researchers and faculty members who come into contact with biohazardous materials to sign an affidavit attesting to the fact that they are not "restricted persons" under the Patriot Act. *E.g.*, www.olemiss.edu/depts/environ-mental_safety/affidavit.pdf (University of Mississippi); www.oseh.umich.edu/-patriot.pdf (University of Michigan).[30]

> [I]nternational-student advisers have been forced into the uncomfortable new role of continuous reporting on our foreign students to the Department of Homeland Security through the new Student and Exchange Visitor Information System, known as Sevis, an Internet-based government-tracking program. While we provide information about those students to the government, we must also serve as their counselors, advisers, and advocates. Balancing those potentially competing roles is far from easy, especially in an enforcement-driven environment.
>
> Sevis has also posed problems because it was rushed into use before being thoroughly tested. Although there have been many improvements, we still struggle daily with inadequate instructions on how to enter required information and apply a one-size-fits-all reporting system to individual students and programs that are anything but alike. When Nafsa: Association of International Educators compiled a summary of its recent discussions with the State Department and the various bureaus of the Department of Homeland Security to help institutions that are struggling with a wide range of Sevis-related problems, the document's table of contents alone ran nine pages.

Sylvia H. Kless, *We Threaten National Security by Discouraging the Best and Brightest Students from Abroad*, CHRON. OF HIGHER ED., October 8, 2004, page B9.

[30] Shortly after the enactment of the Patriot Act at the end of 2001, and just a few months after Capitol Hill was effectively paralyzed by the anthrax attack in September and October, 2001, Congress supplemented the biohazardous materials provision in section 817 by passing the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, Pub. L. No. 107-188, 116 Stat. 594, *codified at* 42 U.S.C. § 300hh *et seq*. The act and implementing regulations mandate additional safeguards governing the use, handling, and transfer of "select agents"—certain biologically hazardous bacteria, viruses, toxins, and nucleic acids. For a good analysis of the 2002 legislation, *see* National Association of College and University Attorneys, *Nacualert: New Regulations on Possession, Use, and Transfer of Biological Agents and Toxins* (January 21, 2003), www.nacua.org/nacualert/docs/-Bioterrorism_Act_Alert_011303_Arial_10pt_squares.htm.

D. ***Critiques of the Patriot Act***

(1) *It infringes civil liberties, particularly the right to privacy and secondarily the rights of assembly and free speech*. This is the most widely expressed criticism of the Patriot Act, best summed up in this fact sheet prepared by the Electronic Freedom Foundation and posted on that organization's Web site at www.eff.org/Privacy/-Surveillance/Terrorism/PATRIOT:

> The USA PATRIOT Act broadly expands law enforcement's surveillance and investigative powers and represents one of the most significant threats to civil liberties, privacy and democratic traditions in U.S. history. …
>
> PATRIOT gives **sweeping anti-privacy powers** to domestic law enforcement and international intelligence agencies and **eliminates checks and balances** that previously gave courts the opportunity to ensure that those powers were not abused. PATRIOT and follow-up legislation now in development threaten the basic rights of millions of Americans. …
>
> Under PATRIOT, civil liberties, especially privacy rights, have taken a severe blow:
>
> - **The law dramatically expands the ability of states and the Federal Government to conduct surveillance of American citizens.** The Government can monitor an individual's web surfing records, use roving wiretaps to monitor phone calls made by individuals "proximate" to the primary person being tapped, access Internet Service Provider records, and monitor the private records of people involved in legitimate protests. …
> - **Foreign and domestic intelligence agencies can more easily spy on Americans.** Powers under the existing Foreign Intelligence Surveillance Act (FISA) have been broadened to allow for increased surveillance opportunities. FISA standards are lower than the constitutional standard applied by the courts in regular investigations. PATRIOT partially repeals legislation enacted in the 1970s that prohibited pervasive surveillance of Americans.
> - **PATRIOT eliminates Government accountability.** While PATRIOT freely eliminates privacy rights for individual Americans, it creates more secrecy for Government activities, making it extremely difficult to know about actions the Government is taking. …

Is the civil liberties critique fair? It emanates from so many different places on the political spectrum and encompasses so many issues and so many provisions in the Patriot Act that an objective answer is difficult given the time constraints of our presentations. But here's one answer—admittedly not scholarly but well-considered. In the fall of 2003 Slate Magazine ran a four-part series timed to dovetail with the second anniversary of the September 11 attacks. The series, titled *A Guide to the Patriot Act: Should You Be Scared of the Patriot Act?*, systematically examined the civil-liberties criticisms leveled at the most prominent features of the Act. The magazine's reporting staff offered this thoughtful conclusion:

> In studying and reporting on the most controversial aspects of the Patriot Act, we have attempted to be as evenhanded as possible. It bears repeating that the Bush administration has fostered a good deal of national anxiety by its simple refusal to release information allaying public fears about how the act is being implemented.
>
> Immediately after Sept. 11, many Americans seemed to fall victim to an understandable fallacy: We believed that by surrendering our freedoms, we were buying national security. Slowly the haze of fear has cleared, and Americans have begun to demand that the freedoms we surrender correspond directly to national security. The parts of the Patriot Act that rankle most are those provisions that sweep normal criminal law enforcement under the looser procedural standards for fighting terror. It's important that the state be able to fight terror. No one disputes this. But it's equally important that the state not use the war on terror to gut the warrant requirement or undermine the First Amendment.
>
> The best check on such encroachments should be a free and objective judiciary. But as we have noted several times in this series, many of the most disturbing Patriot provisions do away with judicial oversight altogether, while others permit judges to act as rubber stamps in *ex parte* proceedings—that is, hearings where only the government side is represented.
>
> The next best check on such encroachments is public scrutiny, and, as we've suggested, that scrutiny is only beginning to be as demanding and impatient as it ought. But most Americans still do not believe that Patriot has in any way affected them. So it's worth noting that many of these provisions are used frequently—even if details are blacked out. ...
>
> We really can be safe without being afraid of our government. It simply requires that security measures be narrowly tailored to fit national security needs. Some parts of the USA Patriot Act meet this test. Some do not. And some are purely opportunistic. Before President Bush convinces Congress to "untie the hands of our law enforcement officials" by expanding the Patriot Act, … Americans need to begin a national conversation about which is which.[31]

(2) *The Patriot Act was a "Christmas tree" bill larded with extraneous items from the law enforcement community's wish list*. One of the most pervasive criticisms of the Patriot Act is that the law enforcement community took advantage of the moment to sneak into the bill many provisions only tangentially related to terrorism. "These

---

[31] Dahlia Lithwick & Julia Turner, *A Guide to the Patriot Act, Part 4: Should You Be Scared of the Patriot Act?* (September 11, 2003), http://slate.msn.com/id/2088239. Links to other three stories in the series are contained in Part 4.

criticisms suggest that the executive branch and sympathetic legislators capitalized on the political aftermath of September 11 to expand executive power by enacting previously blocked legislation only marginally related to terrorism. In sum, the government took advantage of a national crisis to arrogate powers long desired, but politically unacceptable in peacetime." McCarthy, *Recent Development*, 39 HARV. J. ON LEGISLATION at 451.

Is it a fair criticism? Let me respond obliquely by quoting from Beryl A. Howell's recent law review article *Seven Weeks: The Making of the USA PATRIOT Act*, in *The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy & The USA PATRIOT ACT*, 72 GEO. WASH. L REV. 1145 (2004). On page 5 of this outline I described this article as the most detailed legislative history of the Patriot Act available from any non-governmental source. While Howell is not a neutral observer (during Congressional consideration of the legislation that became the Patriot Act he served as one of Democratic Senator Patrick Leahy's principal staff members), he had the benefit of an insider's perspective. Here's what he wrote three years later:

> The administration was not interested in congressional deliberation, compromise, or stopping to discuss details and civil liberties concerns. Instead, it wanted its legislation passed immediately, and if that entailed pressuring Congress with the uncertain threats of future terrorist attacks and telling the public that congressional delay was handing terrorists an "advantage," those were strategies the administration was prepared to pursue. …
>
> The administration's demand for immediate passage of its bill expanding executive branch authority in the form dictated by the administration, and its suggestion that any delay authorizing the powers it sought would imperil American lives, became the mantra of its supporters. This insistence on haste, and unwillingness to expend significant efforts to explain publicly the factual or legal predicates for the demanded expansions of executive branch authority compounded by an apparent disrespect for legislative deliberation and scrutiny, and impatience with civil liberties concerns, created an atmosphere of distrust among defenders of civil liberties and privacy that has dogged the legislation ever since. …
>
> This legislation was never intended to be a substitute for a comprehensive review of the events leading up to the September 11 attacks, or for a more finely tuned legislative response based upon any findings of legal shortcomings that resulted from such a review. … The speed with which the law was enacted, and the importance and complexity of the issues tackled by the USA PATRIOT Act, make it particularly important that government officials in both the legislative and the executive branches engage in ongoing efforts to inform the public about the

substance and effect of the legislation. [72 GEO. WASH. L. REV. at 1161, 1163, 1206-07.]

I take from these passages the following tentative conclusions. The bill was drafted, considered and enacted hastily. Like much of what passes for legislation, it was built from the shards of previous bill-writing attempts. In some respects, it was intended as an immediate, short-term response to the events of September 11. (One of many, I should add: the others included military action against Afghanistan and later Iraq, the detention of hundreds of enemy combatants, and the creation of the Department of Homeland Security.) Congress emphasized the Patriot Act's impermanence by including a "sunset" provision under which many of the legislation's provocative features expire on December 31, 2005. (See the next section of this outline.) It was a sloppily drafted bill, the pieces of which do not fit together coherently. That much is undeniable.

III. WHAT'S NEXT?

A. *Intelligence reorganization.* At the end of 2004, in response to recommendations from the 9/11 Commission and after extensive Congressional debate, legislative gridlock, and intense pressure from organizations representing family members of people who died on September 11, Congress finally passed the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458. This is legislation on a massive scale—several thousand pages long, so long in fact that as of the date this outline went to press the new law hadn't yet been typeset by the Government Printing Office.

The intelligence reorganization bill creates a new National Intelligence Authority headed by the National Intelligence Director ("NID"). The NID would be appointed by the President and confirmed by the Senate, and would have independent oversight authority over more than a dozen intelligence agencies, Most significantly, the NID would be the one government official with comprehensive budgetary authority for all non-military intelligence programs. The NID would also oversee the newly-created National Counterterrorism Center, which would, among other things, serve as the government's primary agency for analyzing and integrating all intelligence pertaining to terrorism and counterterrorism, except intelligence pertaining exclusively to domestic terrorists and domestic counterterrorism.

The bill is designed to augment homeland security in many respects:

- It calls for the development of a plan for the systematic surveillance of the southwest border of the United States by remotely-piloted aircraft and an increase the number of full-time border agents by at least 2,000 a year for each of the next five years.

- It establishes minimum standards for birth certificates and driver's licenses and improves security of Social Security cards.

- It tightens baggage screening procedures and security in screening areas.

- It authorizes funds to improve air cargo security and studies of blast-resistant cargo and baggage containers.

- It mandates strategies to counter shoulder-fired, stinger-type portable weapons, and establishes mandatory minimum sentences for possessing or trafficking in missile systems built to destroy aircraft.

- It criminalizes hoax terrorist threats and giving material support to suspected terrorists.

- In a significant expansion of existing wiretapping authority, it gives the government wiretapping and investigative authority to pursue "lone wolf" terrorists not affiliated with a terrorist group or state.

- It requires the Department of Homeland Security to implement biometric screening for travelers entering and leaving the country.

- In what some critics have described as a gesture to critics, it creates a Privacy and Civil Liberties Board of private citizens, with access to all government agencies, to oversee privacy protections, and recommends increased diplomacy in the Islamic world to combat the spread of terrorism and promote democracy.[32]

High on the Bush Administration's agenda in the next year is the implementation of this gargantuan new law.

B. *Patriot II*. Many of the provisions in the Patriot Act will expire at the end of this year.[33] That fact has led many to anticipate the introduction later this spring of legislation

[32] It's too early for the advocacy community to have prepared comprehensive analyses of the intelligence reform bill. Among the few I found are the following two, each with a decided viewpoint:

- American Civil Liberties Union, *Letter to Congress Regarding Conference Report on S. 2845, the "Intelligence Reform and Terrorism Prevention Act of 2004"* (December 6, 2004), www.aclu.org/SafeandFree/SafeandFree.cfm?ID=17154&c=206.
- Heritage Foundation, *What a Comprehensive Intelligence Bill Should Contain*, September 23, 2004, www.heritage.org/Research/NationalSecurity/bg1799.cfm.

[33] The Congressional Research Service has compiled a complete list of expiring provisions. U.S. Library of Congress, Congressional Research Service, *USA PATRIOT Act Sunset: Provisions That Expire on December 31, 2005* (updated June10, 2004), available on the Web site of the Federation of American Scientists at www.fas.-

[Footnote continued on next page.]

branded "Patriot II"—legislation that would renew some of the sunsetting provisions and add to the Act some items from the Justice Department's wish list.

The Ashbrook Justice Department tipped its hand in early 2003 when it drafted the proposed Domestic Security Enhancement Act. Although the administration bill was never formally introduced, copies were leaked to advocacy groups which promptly posted them on their Web sites.[34] Among the measures in the bill:[35]

- *Secret Arrests.* The bill would overturn a federal court decision requiring the government to disclose the identity of persons it detained in the September 11 investigation. All arrests in connection with "international terrorism" investigations would be secret until the filing of an indictment. "Never before in our history have we permitted secret arrests," says Professor Cole.

- *Ending Consent Decrees Against Illegal Police Spying.* The bill would automatically terminate any consent decree governing police spying that was entered before September 11, 2001, no matter what the basis of that decree. It would essentially eliminate consent decrees for the future with respect to police spying and place substantial restrictions on judicial injunctions.

- *Unchecked Deportation Authority***.** The Attorney General would be given unchecked power to deport foreign nationals whenever their presence is deemed inconsistent with our "national security," which is defined to include "economic interests" or "foreign policy."

- *Stripping Citizenship for Political Associations***.** Citizens could lose their American citizenship on the basis of their political associations. Even activity that is currently *legal* to engage in—for example belonging to or supporting the lawful activities of a group designated "terrorist" by the Attorney General—would be presumptive grounds for loss of citizenship.

- *Bypassing Judicial Oversight***.** The Attorney General could bypass the courts altogether for FISA searches and wiretaps whenever Congress passes a resolution authorizing the use of force.

---

org/irp/crs/RL32186.pdf. The report lists sixteen provisions, among them some of the Patriot Act's most controversial.

[34] *E.g.*, American Civil Liberties Union, *Interested Persons Memo: Section-by-Section Analysis of Justice Department Draft "Domestic Security Enhancement Act of 2003," Also Known As "PATRIOT Act II"* (February 14, 2003), www.aclu.org/SafeandFree/SafeandFree.cfm?ID=11835&c=206.

[35] This section of the outline is drawn from a paper prepared by Georgetown University Law Center David Cole on February 10, 2003. The paper is available online at www.cdt.org/security/usapatriot/030210cole.pdf.

- *DNA Database for "Suspected" Terrorists***.** The bill would authorize creation of a DNA database on "suspected terrorists," expansively defined to include association with suspected terrorist groups.

- *Access to Credit Reports*. Federal law enforcement authorities would be given access to credit reports on the same basis as private companies. Historically, law enforcement access has been more limited for fear that law enforcement is more susceptible to serious abuse than private companies. The bill would eliminate that distinction.

- *Expedited Removal for "Criminal Aliens."* In a provision that arguably has nothing to do with terrorism, the bill creates an "expedited removal" process (with circumscribed judicial review) for any foreign national convicted of a wide range of minor and major crimes, irrespective of when the crime was committed. "This simply exacerbates the already harsh immigration laws governing those who have committed a crime, and seeks to deprive them of any meaningful judicial review, without any connection to terrorism or national security," says Professor Cole.

Look for some or all of these measures to be included in the administration's first draft of Patriot II later this year.