



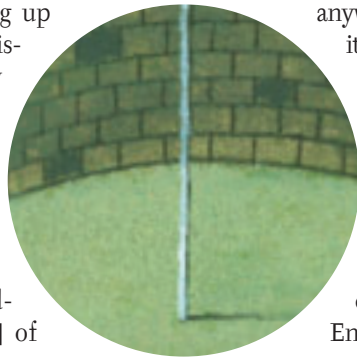
# CIVIL PRIVACY AND NATIONAL SECURITY LEGISLATION: A THREE-DIMENSIONAL VIEW

*Nowhere* in the U.S. Constitution is there a harmonization-of-laws guarantee. As Chief Justice John Marshall famously said in his 1803 *Marbury v. Madison* opinion, which established the principle of judicial review, the Supreme Court is the “final arbiter” of “what the law is.” Thus the task of settling inconsistencies, disharmonizations, and contradictions falls to the Court, which in practice means that many such problems go unaddressed for years and that some cases and controversies are never resolved at all. Of course, the lack of certainty about settling cases may be viewed as one aspect of the observation that democracy can be a complicated and messy process. Such complications, constitutionally thought of as “checks and balances,” are also, however, the beauty of the U.S. constitutional system.

By Tracy Mitrano

*Tracy Mitrano has a doctorate in American history and a juris doctor law degree. She is the Director of Policy for the Office of Information Technologies at Cornell University and the Co-Director of the EDUCAUSE/Cornell Institute for Computer Policy and Law.*

Yet the costs of the checks-and-balances system are sometimes weighed in confusion and consternation against arbitrary and capricious dictates that have the appearance, at least, of resolving conflicts once and for all. An example is the contradiction shaping up between civil privacy legislation (such as the Family Educational Rights and Privacy Act [FERPA] of 1974, the Health Insurance Portability and Accountability Act [HIPAA] of 1996, and the Financial Services Modernization Act [FSMA] of 1999) and national security, information-sharing, antiterrorist legislation (such as the USA-PATRIOT Act of 2001 and the Homeland Security Act of 2002). On the one hand, Democratic administrations have carried forward legislation that prizes the protection of personal data such as educational, financial, and medical records. On the other hand, a post-9/11 Republican administration has championed legislation that enhances the information-gathering powers of the government by expanding its investigatory purview and erasing the liability of private entities who give up information to the government on request. Higher education in general and information technology professions in particular—those who are often the custodians of that data—join with all of American society in an attempt to understand the meaning of these divergent legislative imperatives.



**The**  
 very definition of  
 the word *security*  
 implies that its  
 appropriate  
 function is as the  
 means to another  
 quality and not as  
 an end in itself.

### Privacy and Security

Before delving into a deeper analysis of the legislation, we should pause and examine the terms *privacy* and *security*. The *American Heritage Dictionary* defines *private* as “secluded from sight, presence or intrusion of others . . . to be confined to one person; personal.” Legal scholars have written innumerable books and law review articles about the Anglo-American tradition of “privacy” as encapsulated in

the founders’ framing of the Fourth Amendment and about the expansion of that “right” over time in criminal-procedure jurisprudence.

Though some have pointed out that the word *privacy* never actually appears anywhere in the Constitution, it would be difficult to refute the fact that something of the meaning of the word *privacy* has long resonated in American cultural and legal traditions. Its etymology speaks volumes. *Private* derives from the Middle English *privat*, which comes from the Latin *privates*, which significantly means “not belonging to the state” or “not in public life.” That distinction between public and private is a cornerstone in Western traditions stretching at least as far back as Ancient Greece and Rome and integrated into the Anglo-American culture.

The term *privacy* does not enter the legal lexicon until the end of the nineteenth century, when Louis Brandeis (later a Supreme Court justice) wrote, in a law review article, that privacy “was the right to be let alone.” The use of this term for civil law resonated with early republican principles. That the concept of “privacy” made such a controversial comeback in twentieth-century America should be no surprise. As the American economy shifted from agricultural to industrial, its demographics from rural to urban, its citizenship from categorical (white, male, property-owning) to universal suffrage, and its stature from underdog upstart to world power, relationships of class, gender, race, society, and politics shifted dramatically—and, along with them, the boundaries of what society thinks of as “public” and “private.”

Although most people assume that privacy has grown progressively with American history, it may well be that what has grown are instead the legal definitions of it to compensate for the deterioration of privacy as a cultural concept in the wake

of all this economic and social change. Thus, it is the “expectation” of privacy that is truly at stake—its particular scope and properties within a specific historical context—and not the time-honored tradition of the abstract concept itself.

The word *security* comes from the Latin *securus*, which means “carefree.” Indeed, definitions of *security* often begin with “freedom from danger, risk, etc., safety.” For the purposes of either electronic or national security, this definition reflects far more optimism than anyone can afford. No matter what measures are taken to assert “security” in either realm, no one realistically thinks that the outcome will be complete “freedom.” But notice how the very definition of the word *security* implies that its appropriate function is as the means to another quality—freedom, no less—and not as an end in itself. Balance, of course, is the key, and American history provides us with myriad examples of how that balance has shifted over time.

The Alien and Sedition Acts of the 1790s were the first example of a federal law believed to have thrown off the balance in favor of security over civil liberties. By limiting immigration and naturalization (and thus voting rights), providing the president with sweeping powers to imprison and deport “aliens,” and by creating overly broad prohibitions of free speech, these laws were ostensibly designed to protect the new United States against a purportedly antagonistic French Revolutionary government, but they were interpreted by both contemporaries and historians as legal devices on the part of the ruling Federalist party to silence Thomas Jefferson’s Democratic-Republican party. In short order this attempt backfired on the Federalist party by marshaling support for Jefferson and thus ensuring his “Revolution of 1800” election as president. An 1802 Democratic-Republican-controlled Congress repealed the Naturalization Act and allowed the others to expire. Perhaps more than any other example in American history, this episode stands as a lesson to all of American society about the potential for federal legislative overreach—political impulses of legislation touted as “patriotic” and necessary for national security. The Federal party dissolved after this

debacle, and Jefferson's party remained in power for four more administrations.

Not that all federal emergency legislation has been so easily relegated to the dustbin of history. Nor was such legislation always the "wrong" thing to do. The Civil War could hardly have been fought, or won by the Union forces, without Abraham Lincoln's suspension of habeas corpus, the Anglo-American tradition whereby an imprisoned person can appeal to the highest courts on grounds that the government has violated his or her fundamental civil rights. Another example is Franklin Delano Roosevelt's New Deal legislation. With the very volatile and diverse (left and right) political forces that emerged as a result of the economic depression, this legislation—though at the time exceedingly controversial as a constitutional matter—became the foundation of a regulatory state that defined American society in the second half of the twentieth century and even into the twenty-first. The internment of the Japanese, however, remains the nadir of Roosevelt's emergency measures, the most shameful of all mistaken emergency legislative measures. Thus, each case of "emergency legislation" that protects national security but also curbs civil liberties must be interpreted in the context of very complex history.

### **Civil Privacy Legislation: FERPA, HIPAA, and FSMA**

FERPA, HIPAA, and FSMA share the purpose of preserving the privacy of records, in keeping with the foundational tenets of fair-information practices such as transparency, relevancy, ability to correct the record, institutional obligation to maintain a record of disclosures and provide notice to the subject, and finally, security of those records. Framers of the more recent laws—HIPAA and FSMA—have therefore drawn heavily on FERPA for guidance. In fact, when student records are also medical records, FERPA trumps HIPAA. Under FSMA, if the financial records are already protected under the measures that the institution uses to comply with FERPA, then they automatically meet FSMA requirements. The trick for stewards of that data in colleges and universities is to assess what medical or financial records exist outside of the FERPA framework and then to place them under

that or some other, equally protective administrative umbrella.

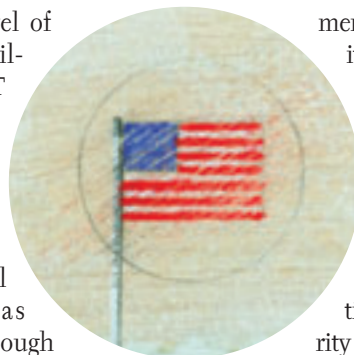
Having dealt with the security of paper documents years ago under FERPA regulations, colleges and universities are now struggling to bring electronic security up to the same level of confidentiality and availability. The creation of IT security programs—which include policies, procedures, and guidelines, risk assessment, and education/training—corresponds to new legal developments such as FMSA and HIPAA. Although they raise the specter of liability, the legal requirements should also come as encouragement and even hope for IT professionals, who have felt they cried in the wilderness for such institutional support for many years. Intrusion-detection and -response plans require leadership, articulated practices, enforceable policies, and education throughout the campus community, all of which include investments in relevant hardware and software as well as in highly trained, full-time employees to address these matters professionally.

### **National Security Legislation: The USA-PATRIOT Act and the Homeland Security Act**

National security, sharing-of-information legislation, such as the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (the USA-PATRIOT Act) and the Homeland Security Act, pulls in a direction contrary to privacy legislation. The USA-PATRIOT Act—well over one hundred pages and passed on October 26, 2001, only six weeks after the events that prompted it—is the longest piece of emergency legislation passed in the shortest period in all of American history. It has three overall goals: (1) to enhance government-to-government shar-

ing of information (by lifting regulations that had monitored law enforcement relations between federal, state, and local authorities); (2) to allow government surveillance and to encourage private entities to share information with the govern-

ment (by alleviating legal liability); and (3) to create and expand existing criminal law designed to fight terrorism (by adding specific provisions and by expanding the definition and powers of existing legislation). The implications of the Homeland Security Act have yet to spell themselves out concretely, so vast is the



**Each case of "emergency legislation" that protects national security but also curbs civil liberties must be interpreted in the context of very complex history.**

reorganization of the federal government under this act, but two pieces are already notably significant. The first is the assumption under the Homeland Security Department of the Immigration and Naturalization Service (INS) and, along with it, the Student and Exchange Visitor Information System (SEVIS) program, which requires colleges and universities to report,

using a government-issued software program, all of their foreign students. The second is the strengthening of penalties for computer abuse and fraud crimes, specifically allowing the death penalty for any abuse (i.e., hacking) that results in serious physical injury or death, regardless of the intention of the hacker (i.e., no evidence of intent to commit a terrorist act is necessary).

The second goal of the USA-PATRIOT Act—government surveillance—and these two aspects of the Homeland Security Act have the most direct impact on scholarship and research, libraries, and IT resources in higher education.

*The PATRIOT Act Amendments FERPA.* The FERPA Act has a "health and safety exception" well-known to student administrators, who invoke it to look at a student's record—for example, in the case where a student is missing and police

hope to find clues to the student's disappearance in e-mail. The USA-PATRIOT Act added a new, "terrorism" exception designed to protect the health and safety of everyone else. For a lower showing than is ordinarily necessary for the government to obtain records under FERPA, law enforcement can pierce the FERPA veil of protection as long as the attesting papers supporting the subpoena claim that disclosure is for the purpose of "a terrorist investigation." Notably, it is narrowly tailored to terrorism.

It is worth noting here the broad definition of *domestic terrorism*: "The term 'domestic terrorism' means activities... [that] involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; appear to be intended (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and occur primarily within the territorial jurisdiction of the United States."<sup>1</sup> Interestingly, the term "appear" is in contradiction to the requisite level of intent in criminal law and that subsection (ii) is so expansive as to include, potentially, matters of civil rights and social change.

The USA-PATRIOT Act has expanded the definition of *domestic terrorism* so broadly that law enforcement now has significant leeway to issue these requests. Still, it is noteworthy that this change in FERPA differs from other USA-PATRIOT Act amendments to existing law insofar as it does require an allegation of terrorism; amendments to the Electronic Communications Privacy Act (ECPA), for example, do not require such an allegation and therefore fall under the four-year "sunset" clause that some legislators attempted to lift in the "Patriot Act II" proposal, which Congress

failed to pass. This narrow tailoring validates the new exception. Thus, college and university counsel should be prepared to review such requests under this new exception and specifically to review supporting papers for the "terrorist" allegations before disclosing the information. Though not specifically required by the USA-PATRIOT Act to keep a record of such requests, custodians of both paper and electronic records might well want to do so, in order to provide the institution with a clear memory of these transactions and to make a record in the event of potential abuse.

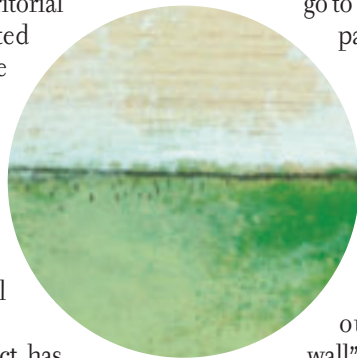
FISA. Of all the PATRIOT Act's new amendments to existing legislation, the most worrisome are amendments to the Foreign Intelligence Surveillance Act (FISA) of 1978. The main thrust of FISA is to circumvent traditional Fourth Amendment requirements of "probable cause of criminal activity" by creating a new standard of "probable cause of a connection to a hostile foreign power." These requests go to a special FISA court, whose papers and proceedings are closed to the public. A special FISA Court of Appeals recently ruled in favor of this new standard and has even eliminated the Justice Department regulations and practices that had previously created a "Chinese wall"<sup>2</sup> separating foreign intelligence investigations from garden-variety criminal ones. The result of these amendments, if not the impact of the USA-PATRIOT Act overall, is the collapse of a distinction between terrorist and criminal investigatory and prosecutorial power.

Specific amendments to FISA have raised concerns. For example, the library community has responded pointedly to a clamp on "free speech" under the USA-PATRIOT Act's "business records 501 section," which amends FISA such that when law enforcement obtains

"business records" (certainly including financial records) from an institution under the FISA standard, the institution will not incur any liability (for example, under FSMA) for the disclosure. The law contradicts fair-information practices of privacy legislation insofar as it does not require the institution to keep a record of the transaction and, most egregiously, prohibits disclosure of even the fact that law enforcement made the request for the information. Once again, college and university counsel should carefully review these requests to be sure that law enforcement specifically grounds the request on 501 provisions, so as to avoid FSMA liability for any other form of improper disclosure of financial records. A record of such a transaction is still advised, notwithstanding the fact that the law does not require it, and most important, all counselors, stewards, and custodians of the data should be informed in advance that these transactions require strict confidentiality. In the name of good planning, FSMA-compliance documents should maintain a section on required disclosures and should outline the specific protocols under this special exception for compliance.

ECPA. The USA-PATRIOT Act amends the Electronic Communications Privacy Act (ECPA) of 1986 in three areas: (1) emergency disclosures; (2) required disclosures; and (3) computer-trespass reports to law enforcement. The first USA-PATRIOT Act amendment of ECPA is uncontroversial. It states that if system or network operators reasonably believe that they have observed information concerning physical injury or death, they may disclose the information to anyone (law enforcement and involved parties). However, the second amendment—required disclosures—presents a controversial constitutional question. Required disclosure refers to what some observers have called "rubber stamp subpoenas," or subpoenas that require neither Fourth Amendment foundation nor judicial oversight and yet may yield law enforcement a considerable amount of information and even content.

The crux of the constitutional question revolves around the difference between conversational detail of telephonic



**Under  
the Homeland  
Security Act, when  
death or serious  
injury results from  
a computer  
compromise, the  
penalty flies all the  
way up to capital  
punishment.**

and of electronic communications. A less-than-Fourth-Amendment standard grants law enforcement, and even third parties such as financial institutions, conversational detail of telephone records, which do not provide content. But the equivalent conversational detail of electronic communications may indeed provide content, particularly in the form of Internet Protocol addresses that resolve to Web pages. It is unclear whether the framers of this legislation understood the technology sufficiently to appreciate the different results and purposely proceeded to lower the bar on content information or whether they did not understand the technology and would not have made the change had they known better. What is clear is that of the many constitutional issues that the new antiterrorism legislation raises, this one is high on the list of civil libertarians. Its debate and jurisprudential conclusions have potentially the greatest constitutional impact on information technology in higher education.<sup>3</sup>

In the third area, the new computer-

trespass amendments allow “owners or operators” of network systems to report incidents of computer trespass (hackings, generally) to law enforcement without liability for disclosure under ECPA. In many ways a “no-brainer”—people call the police all the time when their houses are broken into—this amendment nonetheless presents some complicating questions. For example, when should one report a computer compromise, considering that they happen so frequently? What threshold of damage might make a difference? What kind of control would one need to have in order to contour or terminate an investigation once it has begun?

Three other issues factor into this ECPA amendment. The first is the question of the constitutionality of this provision, since it holds that the alleged perpetrator has “no right to privacy.” Such declaratory statements always make constitutional scholars uneasy, if only because of the idea that it is the Supreme Court—not Congress—that is the “final arbiter” of “what the law is.” The second issue, mentioned above, is the fact that

this provision has nothing whatsoever to do with terrorism. It is no secret that the attorney general’s office had this provision on its legislative “wish list” for some time preceding the events of September 11; the USA-PATRIOT Act simply proved an expedient vehicle by which to enact it. The third point gains particular poignancy in this light. Under the Homeland Security Act, as has been already mentioned, when death or serious injury results from a computer compromise, the penalty flies all the way up to capital punishment. Woe to the defendant alleged to have committed computer abuse. He or she would appear to be without any traditional Fourth Amendment protections and may even face the death penalty.<sup>4</sup>

#### *Homeland Security*

The principal thrust of the Homeland Security Act is to reorganize a significant chunk of the federal law enforcement and immigration and naturalization bureaucracy under the roof of one central federal agency. This thrust grew out of the concern that the compartmentalization

of federal intelligence and law enforcement structures did not permit adequate study and forewarning, which might have prevented the terrorist attacks of September 11. Much remains to be done on this reorganization. Little definition is available because appropriations for the project are occurring contemporaneously; implementation is therefore largely prospective at this time. The old axiom about power corrupting and absolute power corrupting absolutely comes to mind, however, as one contemplates the reach of this agency. The American Revolutionaries and the constitutional framers, whose greatest concern was the accumulated powers of a centralized government, would be challenged by these changes, although it is important to remember that the United States of America is hardly the same backwater upstart of imperial British power that it was in the late eighteenth century. It is now an imperial power in its own right, and history teaches us that imperialism requires centralized power.

Yet the Homeland Security Act has already had an impact on immigration. For example, the Student and Exchange Visitor Information System (SEVIS) is a mandatory, government-issued software program that tracks the whereabouts of visiting foreign students in U.S. colleges and universities. Although it has received extensive attention as a result of the circumstances surrounding the events of September 11, the general concept of tracking all visiting foreign students is not new. Rather, it has long been a part of INS law that fell into widespread disuse as a result of bureaucratic disorganization in the INS. The USA-PATRIOT Act therefore echoed existing INS law to require mandatory reporting, and the Homeland Security Act passes that same baton forward.

The most obvious problem with SEVIS thus far is that it is an exceedingly faulty piece of software. Technical problems are commonly and widely noted, including the inability to clearly communicate with the new Homeland Security Office in charge of tracking reports from individual colleges and universities and even including such egregious gaffes as documents from one institution mistakenly being directed to other institutions instead of to the Washington office. Im-

plementation schedules have also been exceedingly unrealistic and have twice been revised. And then there are the legal questions about the impact of SEVIS. For example, is it a violation of FERPA? The answer to that question will depend on the kind of information fields that the Homeland Security Office requires campuses to fill out in these forms. Another question is whether FERPA even applies to foreign-exchange students.

Owing to the enormous bureaucracy that has grown up around all of immigration, a bureaucracy of which SEVIS is just one piece, foreign students and scholars often wait interminable periods for clearance to the United States. Some give up completely or find that their graduate professors have had no choice but to turn research or postdoctoral projects over to available personnel. The jewel in the crown of American society, U.S. higher education cannot long survive as the envy of the rest of the world when the rest of the world is hardly allowed to participate in it.

### The Relationship between Privacy and Security Legislation

Civil privacy legislation that includes security measures—legislation such as FERPA, HIPAA, and FSMA—should be the rule. National security, sharing-of-information, antiterrorist legislation—such as the USA-PATRIOT Act and the Homeland Security Act—should be the exception. According to long-standing principles of constitutional law and to more recent principles of civil privacy legislation, only with proper showing on the part of law enforcement should breaches of these privacy rules be allowed. Given the USA-PATRIOT Act departures from traditional constitutional standards, many people are concerned that the exceptions may soon swallow the

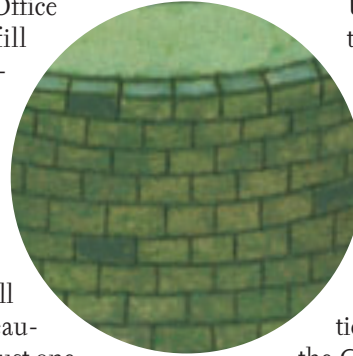
rule. The tension between these two types of legislation speaks to the more general concern of American society at large about a diminution of privacy overall, whether caused by changes in the law, in social norms, or in the very nature of information technologies.

Underlying this tension is the more specific confusion that has arisen between electronic security and national security. Appropriations bills for research on cybersecurity mark one example of a proper intersection of electronic security and national security. For example, the Cybersecurity Research and

Development Act of 2002 “authorizes \$903 million over five years for these new programs, to ensure that the U.S. is better prepared to prevent and combat terrorist attacks on private and government computers.”<sup>5</sup> Another example of an appropriate merging of the two security arenas is the Research and Education

Networking Information Sharing and Analysis Center (REN-ISAC), the organization that “supports higher education and the research community by providing advanced security services to national supporting networks.”<sup>6</sup> Such measures should be supported enthusiastically, across the board politically, and in the name of all that the United States, and U.S. higher education, stand for: the highest academic standards in the world.

Yet simply because electronic security and national security enjoy some synergies does not mean that they should become synonymous. As we have seen, the security component in privacy legislation such as FERPA, HIPAA, and FSMA acts as one of several fair-information principles. It is a means to an end. As the old adage goes, “You can’t have privacy without security.” But security in the sense of the current strategies for ensuring national security presents a very different and contradictory dynamic. The



**Simply**  
because electronic  
security and  
national security  
enjoy some  
synergies does not  
mean that they  
should become  
synonymous.

sharing-of-information theme of the USA-PATRIOT Act imposes the opposite of privacy by creating a one-way flow of information, from citizens to the government. The erstwhile Total Information Awareness Program is perhaps the best example. This program was planned to monitor all electronic communications with an algorithm designed to ferret out “terrorists.” Yet for many people, on both the left and the right of the political spectrum and just about everywhere in between, it encapsulated the worst fears of omnipotent government surveillance. That the government is currently reconfiguring this program, as the Terrorism Awareness Program, speaks to the tenacity with which the administration of George W. Bush has shaped domestic strategies for national security as an end rather than as the means to preserving civil liberties.

In this concept of national security, security no longer augments privacy but is pitted against it in a zero-sum competitive game. What is the effect on colleges and universities? How do the current

strategies for national security stack up against the mission of higher education? At the very least, the answer is problematic. The new exception to FERPA came about because of the vast FERPA abuses that occurred in the immediate aftermath of 9/11. Federal law enforcement issued verbal requests for educational records, without the proper showing of compulsory legal papers, and a number of schools complied. FSMA and HIPAA have not been in force long enough to test their mettle against encroachment, but the lowering of constitutional standards and the elimination of liability for private entities under the USA-PATRIOT Act create all kinds of new legal opportunities to undermine the purpose of that legislation, if not all communications privacy as it has been defined legally at least since the late 1960s.

The bureaucratic restriction on the use of “select agents” under the USA-PATRIOT Act has resulted in a massive scaling back of academic research. At Cornell University, for example, eighty-three research projects used select agents

before the USA-PATRIOT Act; only three of these projects remain. Immigration and naturalization law, now under the Homeland Security Office, has made the visas for foreign students so burdensome that many have their academic projects delayed or even suspended completely. Some have entirely given up their hopes of coming to the United States for academic work. And those same restrictions have made it nearly impossible for academics from around the world to enter the United States for collaboration, consultations, and conferences. As a result, American higher education is becoming an increasingly isolated and parochial environment in which to conduct research and inquiry—the very opposite of the open, international dynamic that made it so vital in the twentieth century.

Privacy is a constitutional principle because the nation’s founders believed it was a necessary ground for the development of responsible, autonomous citizens in a democratic republic. Just as under the U.S. federalist system “individual rights” become intertwined with

“states’ rights,” so might it be argued that privacy principles underwrite the foundational autonomy of higher education institutions as distinct entities in American society, separate from both the government and the market. Higher education joins with government and market forces to fight terrorism. But in doing so, colleges and universities should be careful to maintain distinctions. “Electronic security” should not be conflated completely with “national security.” Academic research should not be confused with “bio-terrorism.” And a careful watch over the country’s borders should not resolve to blanket suspension of foreign travel to—or study in—the United States.

How hackneyed the old adage “those who neglect history are condemned to repeat it,” but how true that adage rings in these anxious and troubling times. Admittedly, no one has the crystal ball to tell us what balance of civil privacy and national security measures will optimally protect us in an unknowable future. Clouding the future further is the fact that a two-dimensional view of “civil pri-

vacancy versus national security” hardly represents the full, three-dimensional quality of what is at stake for all of American society. The best we can hope to do is to remain aware and to address discrete issues as they arise. For example, colleges and universities should insist on being presented with compulsory legal papers, in proper order, before disclosing information to law enforcement, and they should maintain records of those transactions regardless of relaxed standards under antiterrorist legislation. National organizations supporting higher education—organizations such as the American Association of Universities (AAU) and the American Association of University Professors (AAUP)—should continue, as they have already begun, to place pressure on the appropriate authorities, for example, the Education Department and the Homeland Security Office, to address the adverse impact that new restrictions are having on collaboration and research. Without these measures, current strategies of national security may well be on the way to undermining the open and

democratic spirit of American higher education. Security without freedom is no security at all, and it is in precisely this state that we will ruefully recognize that the terrorists have won after all. *e*

#### Notes

1. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001*, H.R. 3162, title VIII, section 802.
2. In the legal profession, “Chinese wall” is a term used to signify the separation that a law firm, for example, would create between different sections of practice to avoid potential conflicts of interest.
3. The “rubber stamp subpoena” issue arises under FISA as well as ECPA. Thus the significantly lower standards by which law enforcement can obtain content data under these surveillance provisions, combined with the special constitutional complications of FISA and the broad definition of *domestic terrorism*, add up to significant departures from traditional Fourth Amendment civil liberties.
4. See Cornell University’s “Procedure and Protocols under the ‘USA-PATRIOT Act’ Exceptions to the Electronic Communications Privacy Act,” <<http://www.cit.cornell.edu/oit/policy/memos/PatriotAct.html>> (accessed August 26, 2003).
5. House Committee on Science, “Congress Bolsters Nation’s Defenses in War on Cyberterrorism,” press release, November 12, 2002, <<http://www.house.gov/shays/news/2002/november/science.pdf>> (accessed August 21, 2003).
6. See <<http://ren-isac.iu.edu/>>.