O nly forty-five days after Sep-

tember 11, 2001, the USA PATRIOT Act, formally enti-
titled the Uniting and Strengthening America by Providing Ap-
propriate Tools Required to Intercept and Obstruct Terrorism, was enacted into law. In brief, the act expands the use of surveillance devices from telephone sys-
tems to electronic communications, low-
ers the standards required in order to use such devices, and may override existing liberty confidentiality laws.1 Eight months later, in May 2002, Attorney Gen-
eral John Ashcroft issued guidelines making it easier for federal investigators to continue even without evidence of criminal activity. In the end, these guidelines led the FBI to conduct investigations using highly intrusive techniques for up to one year with no oversight from FBI head-
quarters and even if an investigation is turning up no reasonable indication of criminal activity. These changes to the federal legal landscape are significant, as they will have far-reaching ramifications for years to come in the areas of security and privacy, in ways that will fundamentally affect the academic enterprise.

The New Horizons department in EDUCAUSE Review is about new and in-
novative technologies. In this issue, we want to raise awareness of the impact that this new federal legal landscape will have on higher education and on how colleges and universities use technology. This is a challenging task, because it requires that academic administrators and policy-
makers understand and synthesize massive am-


T he new USA PATRIOT Act reopens the possi-

bility for higher education institutions, as well as In-

ternet Service Providers, to hand over

“voluntarily”—substantial information

about potential information in the

form of student identifications and

other information—and to do so without any voluntary provision of such information without a court order or any legal instru-

ment was often illegal. In addition, the act dra-
matically expands the records that the government can request with a simple subpoena (without court review) to in-
clude session records, network log ad-

dresses and routes, credit and bank infor-

mation and other means of payment, and

so on. Institutions may want to document how this information is organized, both centrally and on subunit and departmen-
tal systems, in cases where they need to re-

spond to a comprehensive request.

5. Portals. Portals are becoming increas-
ingly popular and useful. The more cus-
tomized and personalized the portal sys-

tem, the more effectively it provides informa-
tion tailored to the individual. Unfortunately, this makes portals espe-
cially vulnerable to content tracking. Un-

like other areas, where tracking informa-

tion may be summarized broadly, the use of portals is much more intimate—can be tied to activity that is truly life-threatening, there are two issues for the academic commu-
nity here. First, what role does the college

or university play in evaluating how its

information intersects with these technologies in


campus and complex and sometimes unpredictable

ways that threaten to temper the continued

teaching, learning and research. As we will high-

light, privacy concerns and new legal re-
orneratives of gathering computer infor-

mation intersect with these technologies in

ways that threaten to temper the continued

teaching, learning and research. As we will high-

light, privacy concerns and new legal re-

quirements are beginning to change the tech-

niques and policies regulating computer infor-

mation and other means of payment, and

so on. Institutions may want to document

© 2002 Paula T. Kaufman and Peter M. Siegel

New Horizons

9/11: Legislation and Technology: The Academic Impact

By Paula T. Kaufman and Peter M. Siegel

1. Routine Academic Data. Although no one wants to aid terrorist activities, recent government practice will likely funda-

mental changes in how higher education and on how colleges

and universities use technology. This is a

challenging task, because it requires that academic administrators and policy-
makers understand and synthesize massive am-


T he new USA PATRIOT Act reopens the possi-

bility for higher education institutions, as well as In-

ternet Service Providers, to hand over

“voluntarily”—substantial information

about potential information in the

form of student identifications and

other information—and to do so without any voluntary provision of such information without a court order or any legal instru-

ments. First, as each higher education institution

will have to be aware of how to respond to law-enforcement re-

quests, including training in advance for those institutions, and for academic and other staff who may be asked directly and

immediately to provide information.

Lastly, and as good citizens, often want to be responsive to outside agencies and law enforcement, so they need to know what is expected of them and how to deal with these requests in a manner consistent with what is expected of their institutions.

Second, colleges and universities must consider the implications of these laws to the extent that they may be used in concert with other data to determine individuals’ location...