FERPA Obligations and the USA Patriot Act

In response to the September 11 terrorist attacks on the World Trade Center and the Pentagon, Congress enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorists Act, commonly known as the USA Patriot Act. Among the Act's provisions are several which have a direct impact on colleges and universities, including specifically their obligations with respect to student "education records" under the Family Educational Rights and Privacy Act ("FERPA"). Just a few weeks ago, LeRoy Rooker, Director of the U.S. Department of Education's Family Policy Compliance Office issued a guidance ("Guidance") discussing the impact of these statutory changes on an institution's FERPA obligations. The Patriot Act also impacts colleges and universities in their role as providers of "communication services" (*i.e.*, telephones, computers and Internet access). This Information Memo discusses the effect of the Patriot Act on colleges and universities in these two key areas.

FERPA Obligations and the USA Patriot Act

FERPA essentially prohibits federal funding for any college or university that has a policy or practice of disclosing a student's "education record" without the consent of the parent or student, as appropriate. Education records are broadly defined to include "records, files, documents and other materials which (1) contain information directly related to a student; and (2) are maintained by an education agency or institution or by a person acting for such agency or institution." Subject to certain exceptions, FERPA requires prior written consent from the parent or student before personally identifiable information from education records can be disclosed to a third party. Among the 16 exceptions to this requirement which exist, one involves responses to lawfully issued subpoenas and court orders, and a second involves health or safety emergencies.

Even prior to enactment of the Patriot Act, the subpoena/court order exception applied in three contexts. First, an institution could (and still can) disclose education records to anyone designated in a federal grand jury subpoena, and that subpoena can lawfully order the institution not to disclose to anyone (including the parent or student) either the existence or contents of that subpoena or the institution's response to it. A second, similar exception exists permitting responses to any other subpoena issued for a law enforcement purpose, which, for good cause shown, can also include a non-disclosure order. When such a subpoena is issued by an agency, as opposed to a court, the institution may request a copy of the "good cause" determination. In the case of any other subpoena, however, an institution may disclose education records only if it makes a reasonable effort to notify the parent or student of the order or subpoena in advance of compliance, so that the parent or student can seek protective action.

The "health or safety emergency" exception permits non-consensual disclosure of education records (including personally identifiable, non-directory information from education records) if knowledge of the information requested is necessary to protect the health or safety of the student or other individuals. This exception has been narrowly construed, has been temporally limited to the period of the emergency, and only covers that information related to the emergency; it does not allow for a blanket release of personally identifiable information from a student's records. In the weeks immediately following the September 11 attacks, hundreds of colleges and universities received requests for information about foreign students, without supporting subpoenas. The U.S. Department of Education's position was, and as is made clear in its recently issued Guidance still is, that this exception applies in cases such as the September 11 attack itself, but any release of information, even in those circumstances, "must be narrowly tailored considering the immediacy, magnitude, and specificity of information concerning the emergency." Ongoing investigations into terrorist activities generally are not likely to fall within this exception due to the absence of immediacy and specificity.

The Patriot Act amends FERPA in a significant way to make it easier for law enforcement officials to secure, and therefore for institutions to release, education records without student consent. Under the amendments, the Attorney General, or designee, may now obtain an *ex parte* court order requiring an institution to turn over education records relevant in a terrorism investigation. An *ex parte* order is one issued by a court without notice to an adverse party. Not

only can the order be obtained *ex parte*, but the institution can turn over the requested records without the consent of, or even notice to, the parent or student. In addition, the amendments provide that an institution is not required to even record the disclosure of this information, as it is required to do in other disclosure circumstances. Providing further protection to institutions, the amendments expressly provide that an institution "shall not be liable to any person" for good faith disclosure of education records in response to such an order. Thus, not only is the institution given clear protection from Department of Education action but also protection from any private cause of action that might otherwise have arisen from the disclosure. One indirect impact of this amendment is that it makes it even clearer that institutions should not be providing such information in the absence of a court order.

Of course, even without the amendments, nothing in FERPA prohibits school officials from contacting authorities to report firsthand information which is not part of an education record. Thus, the Guidance expressly recognizes the appropriateness of a school official advising law enforcement officials of suspicious behavior or activity based upon direct observation or personal knowledge. In addition, an institution may disclose to authorities requested "directory information" from education records without prior parent or student consent, provided it has given students notice of its directory information policy and an opportunity to opt out of having their directory information disclosed. Directory information includes, but is not limited to, a student's name, address, telephone listing, electronic mail address, photograph, date and place of birth, major field of study, dates of attendance, grade level, enrollment status, participation in officially recognized activities or sports, weight and height if a member of an athletic team, degrees, honors and awards received, and the most recent education institution attended. Institutions, however, must be careful not to combine directory information with an impermissible disclosure of non-directory information. As the Guidance points out, while an institution may respond to a request for directory information on *all* students, it may not provide that same directory information on students of a certain race, gender or national origin, because that race/gender/national origin identification is itself non-directory information.

The Impact of the Patriot Act on Institutions Which Provide Communication Services

Title II of the Patriot Act, entitled Enhanced Surveillance Procedures, gives the government expanded opportunities for securing information through warrants, subpoenas and court orders. Specifically, it allows for access to stored voice-mail messages without specific wiretap authorizations and adds categories of customer information which can be provided in response to administrative subpoena (*e.g.*, subscribers' local and long distance telephone connection records; subscriber identity information; subscriber payment information; records of session times and durations; and length and types of service). The amendments also enhance authorities' ability to secure Internet address information and Internet surveillance.

While these are significant amendments in terms of increasing the government's access to information, from an institution's compliance perspective this increased access still requires a warrant, subpoena or order. What institutions may notice as a result of these changes, however, is an increased frequency of government requests for information and shorter time frames for responding.

On the other hand, other provisions of Title II permit providers of electronic communication services to voluntarily disclose certain information to law enforcement officials. Specifically, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury requires disclosure without delay, the contents of an electronic communication may be disclosed to law enforcement officials. Similar disclosure of information about a "customer" or "subscriber" in emergency circumstances can also be made. These voluntary disclosure provisions expire in 2005, unless extended by Congress.

Foreign Student Monitoring

Within the past few weeks, Congress also passed The Enhanced Border Security and Visa Entry Reform Act of 2001. This legislation requires institutions to put into place an interim tracking system on all F, J and M visa students. The

specific impact of this legislation is beyond the scope of this Information Memo, but it will be the subject of one to follow shortly.

Conclusion

It certainly is not surprising that the events of September 11 were followed by legislation enhancing the ability of law enforcement officials to gather information on foreign students in the United States, nor should we be surprised to see the enactment of additional legislation in this area in the coming months. Now more than ever it is prudent for institutions to designate a single individual on campus to coordinate all law enforcement information requests and to create a protocol to guide responses to those requests. Because these requests may extend beyond traditional "student records," government requests for information may be made directly to security, human resource, computer and information services and academic departments, making it that much more important to have a centralized resource to oversee responses. In addition, an institution's privacy policy, especially as it relates to computer use, should be reviewed to make sure that it does not overstate users' expectation of privacy. Institutions should also keep a confidential log of requests received and responses provided, so that if issues later arise with respect to the appropriateness of the institution's actions, there is a record of what the institution did and why.