

MAY 8 [2008]

## When FERPA Affects IT

In late March, when the U.S. Department of Education released its proposed changes to regulations that govern the Family Educational Rights and Privacy Act, most of the attention focused on the latitude granted (or, in some cases, reiterated post-Virginia Tech) to college officials for determining in what circumstances and to whom students' information could be disclosed. Since then, both offline and in online list discussions, information technology and network security officers have debated the impact of the rules on more mundane — but potentially just as relevant — functions of colleges' day-to-day operations.

Those discussions shifted to a more formal venue on Wednesday at Educause's annual policy conference on the federal information technology agenda for higher education. The nonprofit group, which supports the "intelligent use of information technology," was finalizing its own recommendations to the Education Department, due today, that would be included along with other signatories in an umbrella document from the American Council on Education. At a morning session called "The IT Implications of Proposed FERPA Regulations," officials from several organizations discussed an overview of the potential changes, offering in some cases minor tweaks — and in others, major criticisms — of specific rules.

Much of the discussion centered on what colleges elect to publicize as directory information. As defined by current regulations, "directory information" that "would not generally be considered harmful or an invasion of privacy if disclosed" — assuming students have been notified upon enrollment and can opt out of disclosure — includes names, addresses, phone numbers, e-mail addresses and photos. Other private data, such as grades and disciplinary history, cannot be included in directory information, whether accessible freely online or not.

Until now, the rules haven't specified whether students' Social Security numbers, and the proprietary ID numbers many colleges assign to students, fall into the "directory information" category. The proposed changes specifically bar both numbers from that designation, which many officials have called a commonsense step but that may also result in unintended effects.

"SSNs and other student ID numbers are personal identifiers that are typically used for identification purposes in order to establish an account, gain access to or confirm private information, obtain services, etc. The proposed regulations are needed to ensure that educational agencies and institutions do not disclose these identifiers as directory information, or include them with other personally identifiable information that may be disclosed as directory information, because SSNs and other student ID numbers can be used to impersonate the owner of the number and obtain information or services by fraud," according to the department's proposed rules.

But, they continue, “The proposed regulations are also needed to clarify that unique personal identifiers used for electronic communications may be disclosed as directory information under certain conditions.”

That caveat reveals a distinction in the rules between a “student ID” and “user ID” — a distinction that at many colleges may not exist. “Different institutions use them in different ways, and so we’re trying to make sure that the way that the institution uses the student ID is taken into consideration in whether it’s appropriate” to disclose or not, Ada Meloy, the American Council on Education’s general counsel, said in an interview.

Under the proposed changes, a student ID is treated like a Social Security number and cannot be disclosed in directory listings; a “user ID,” by contrast, is legitimate “directory information” that cannot be used to obtain private data except “in conjunction with one or more factors that authenticate the student’s identity.”

“We have a long history in our office of saying that student ID numbers may not be disclosed ... that they’re like SSNs,” said Frances Moran, program specialist at the Education Department’s Family Policy Compliance Office, at the session. But “things have changed,” she said, and the department has recognized that if an identifier acts essentially “like a name,” it alone would not pose a breach of privacy and could be disclosed. What exactly a “student ID number” is will be defined in the final version of the updated regulations, she said.

Some officials, however, don’t agree that student ID numbers, whatever they look like, should be elevated to the level of a Social Security number. Barmak Nassirian, associate executive director for external relations of the American Association of Collegiate Registrars and Admissions Officers, called the rule distinguishing student IDs from user IDs a “dogmatic statement.” “After all, when are student IDs used by themselves?” he said at the session. Similar concerns from IT security officers have echoed that complaint. Some have wondered, for example, if the rule would forbid professors from publicly posting grades by students’ ID numbers in order to conceal their names.

Others worry that the regulations are unclear in cases where a “student ID” is the same as the “user ID” that students use to log in to university Web sites and online services. Partially, the distinction boils down to authentication as opposed to identification; the former ensures that the right person is certified to view private information, while the latter merely determines one’s identity for login purposes. Having an identification number, without any other verifying information, doesn’t necessarily ensure that a person is who she says she is. But for some colleges, the two have collapsed into a single identifier that may not apply to the distinctions made by the proposed rules.

Nassirian said he agrees with the spirit of the regulation but that the wording (“user” as opposed to “student,” for example) is misleading. “I think that’s a semantic issue, but that has to be clarified,” he said later in an interview.

At the Educause session, he also stressed his belief that the new regulations did not go far enough in safeguarding personal information that colleges send to outsourced service providers. In the interview, he said he worried that such providers could potentially share data with each other, creating “secret databases” unknown to the original owners of the data. The

worry, he said, was that companies could “basically run secret registrar shops where those data continue to exist and continue to be disclosed ... that’s the problem here.”

According to Moran, the final regulations are due at the Office of Management and Budget by the end of August, and approval could possibly take until mid-December of this year.

— **Andy Guess**