The Roads Ahead

Policy issues originate in many ways, in many venues, and for many reasons. Some persist and evolve. Others come and go—and then sometimes come back again. In some cases we can anticipate what will become important; other times we’re taken by surprise. That’s as true for IT issues as it is for anything else in higher education.

Many of us believed, for example, that the copyright/peer-to-peer negotiations around the U.S. Higher Education Opportunity Act regulations in 2009 had put that issue largely to rest. Instead, infringement issues have required constant attention as the entertainment industry pursues a broad array of filtering and response initiatives. (These aren’t focused on higher education, as the HEOA regulations were, but they nevertheless affect colleges and universities.) For a different example, we hadn’t expected the Commerce Clause—specifically, how it might relate to one state’s regulation of network-based education originating in another state—to require attention. Yet as questions about for-profit nontraditional education converge with intrastate financial challenges, it has. What authority does Kansas, say, have to regulate degrees granted in Colorado’s online programs? Should the U.S. Department of Education take a stand on such regulation? If so, how should it balance the interests of Kansas and Colorado?

Hard as it may be to anticipate which policy issues will emerge when, in what form, for what reason, and with what persistence, it’s nonetheless important to try. Moreover, it’s important to think about policy issues not only in isolation but also as an aggregation embodying synergy and contradiction. We in higher education need to share our thinking about policy. We need to keep it up-to-date.

Listed here, in no particular order, are some policy issues we think may be important to higher education IT practice in the coming year. We hope this list will help generate discussion, argument, and insight and will help the higher education community anticipate the potholes in the IT policy roads ahead.

**Social networks and privacy.** As communication and collaboration within and across colleges and universities incorporate services such as Google Docs, Microsoft Office Live, and Facebook, institutions lose the ability to directly enforce compliance with privacy regulations, policies, and expectations—or even to monitor compliance. This can lead to unpleasant or dangerous interactions between community members, to undesirable or unlawful exposure of personal and institutional data, and even to institutional liability.

**Identity management.** Higher education has long been a leader in securing and integrating identity management within and between campuses. As identity, access control, and especially identity management federation become national issues, emerging standards and requirements need to be coherent rather than vary from organization to organization. They should be compatible with campus practice and should benefit from campus experience.

**Blended and online learning.** How should moving beyond traditional classroom-based educational models alter administrative concepts such as “contact hour,” “headcount,” “full-time,” and “attendance”? Since much educational financing entails detailed metrics based on these attributes, policy questions emerge on how to translate them from historical to future practice.

**Affordability.** Requirements that students own computers and access network-based resources have been criticized for making education inaccessible to some students. Today, computers and network resources are praised for enabling access for all students. How technology affects educational costs—to both institutions and students—requires careful analysis, especially as financial-aid policies accommodate new teaching and learning models.

**Accessibility.** There is increasing pressure for campus web pages and instructional materials to conform to existing and emerging federal accessibility standards, especially for the blind. This has profound and expensive implications for the design and maintenance of campus web pages and especially for media-intensive, web-based instruction. Compliance requirements will even affect the selection of commercial e-readers, software systems, and cloud computing services.

**Assessment.** As education expands to include different styles of learning and broader goals, assessing outcomes and using learning analytics to individualize instruction become more important. Policy issues arise as data-collection methods and monitoring implicate Fair Information Practice Principles and as assessment data drive resource allocation, performance appraisal, and other organizational choices.
Law enforcement and counter-terrorism. Law enforcement and national-security entities seek broader regulation of and access to network traffic. This may result in legislation and/or regulations that require campuses to facilitate law enforcement’s ability to “tap” communications without campus staff involvement, perhaps with fewer procedural safeguards or ones different from those currently in place.

Export controls. Some agencies seek to restrict access to certain applications, data, computers, technologies, or networks with perceived national-security implications. These restrictions involve a variety of regulatory frameworks. Campuses might need to restrict access for certain individuals (e.g., non-citizens or citizens born abroad) and to constrain the contents of laptops or storage devices carried across borders by traveling faculty and staff.

Access requirements for research data. Federal granting agencies are not consistent in how they define and govern research-based intellectual property, especially electronic datasets. Increasingly, agencies require contractors and grantees to make the intellectual property resulting from federally funded research available to other researchers or to the public. But each agency has different requirements. Consistent policy for definitions and access would greatly simplify compliance with data-access requirements.

Data management. As requirements proliferate to preserve data and make it available, even after expiration of a grant, we need to clearly define responsibility and governance. The financing of long-term data storage and access and the privacy, confidentiality, security, and other issues arise around security mechanisms, repository types, and requests for access.

Breach response. The definition of a “breach” of personal information varies across states and across campuses. How campuses respond also varies. Congress has considered extending Federal Trade Commission jurisdiction to include higher education. This might entail new requirements and liability, a problem perhaps counterbalanced by the elimination of state-by-state variation.

Longitudinal tracking. Statewide longitudinal data systems centrally document students’ progress through high school. They are proliferating, particularly as federal and other funding becomes tied to persistence, performance, and graduation. In some cases, state data systems are broadening to include college entry and progression. This triggers policy problems such as ensuring security and privacy and standardizing unit values and attendance status across diverse public and private colleges and universities.

Network neutrality. Higher education benefits when public networks behave neutrally with respect to the origin, destination, and content of network traffic. How best to achieve network neutrality, given its very real political, technical, and financial challenges, remains a complex question. Higher education needs to frame its positions clearly and effectively if we are to influence the outcome.

National Broadband Plan. As campus-based programs give way to programs focused on students who study from home or the workplace, it becomes critical that homes, libraries, and other likely venues for learning be equipped with affordable, high-speed networking.

E-Rate/Universal Service Fund. This long-standing program taxes phone bills and uses those funds to subsidize rural phone service. There are proposals to broaden the tax base for the program and to expand its subsidies to include broadband services and anchor institutions. These changes might be very costly and/or beneficial for various colleges, universities, and collaborative networking ventures.

State regulations and procurement. Tension continues as states desire to run campus information technology as part of statewide economy-of-scale initiatives and as campuses desire more autonomy and procurement authority. This is especially important during the present economic crisis as states seek areas where they can achieve greater efficiencies and reduce costs.

Rethinking use policies. Many campuses are revising their acceptable-use policies (AUPs) to address increasingly pressing problems such as cyberbullying, “commercial” use for private gain, diversion of campus resources to outside entities (e.g., Skype supernodes), and copyright compliance. Others are creating dedicated facilities to accommodate desirable uses not sanctioned by regular AUPs, such as guest access to wireless networking.

Policy development and compliance roles. On many campuses, responsibility for privacy, security, and other campus IT-related policies has evolved into a shared model involving close collaboration between IT units and other campus units. This can include quasi-autonomous positions entitled Chief Information Security Officer, Chief Privacy Officer, or Chief Compliance Officer—whose reporting lines bypass the central IT organization. In some cases this works well, and in others it promotes inefficiency and inconsistency.

Outsourcing and cloud. There are good economy-of-scale and standardization reasons to outsource, and there are excellent providers offering such services. Moving applications and data outside direct campus control raises privacy, security, and business-continuity issues. Contracts between campuses and providers can affect these for better or worse.

Not all of these issues will become important in the next year. Some may never become significant, and some new ones will join the list. We in the EDUCAUSE Washington, D.C., Office will tackle these issues as they arise. We welcome your comments, advice, and support as we do so.

Greg Jackson ([gjackson@educause.edu]) is Vice President for Policy and Analysis, Rodney Petersen ([rpetersen@educause.edu]) is Senior Government Relations Officer and Managing Director of the Washington Office, and Steve Worona ([sworona@educause.edu]) is Senior Policy Director at EDUCAUSE.