Tracking Policy Cycles

Few policy issues are entirely new, even fewer vanish permanently, and most cycle—that is, their importance waxes and wanes, sometimes rapidly and sometimes glacially, as they are affected by technology, society, or politics. If we understand how policy challenges evolve, then in principle we can anticipate when different issues will become important and how to address them. The Policy Matters department in EDUCAUSE Review seeks to achieve this understanding for federal, state, and institutional policy issues affecting higher education information technology.

Two pairs of policy issues illustrate how policy evolution varies. In each pair, one set of policy issues evolves continuously, and the other evolves discontinuously. The first pair contrasts the policy evolution around copyright and cloud services, and the second focuses on data-management policies in social networking and institutional databases.

Copyright and the Cloud
Copyright currently attracts policy attention for at least two reasons: (1) the “peer-to-peer” provisions in the recent Higher Education Opportunity Act, and (2) Google’s Book Search project. Peer-to-peer compliance issues should quiet down as best practices evolve, and Google-related issues should subside as lawsuits are resolved. This suggests that copyright will become relatively dormant as a policy issue.

But the opposite is more likely: the current copyright issues are actually woven together in a subtle fabric, and their inevitable cross-stitching will bring the copyright question back to the forefront. Today’s copyright principles and rules emerged to protect hard-to-reproduce physical books, records, and movies, and they simply cannot extend smoothly to intellectual property that has no physical or temporal boundaries. As Larry Lessig argues in his article in this issue of EDUCAUSE Review, the substance of policy discussion will eventually shift sharply from today’s focus on compliance and control to a radical reframing of the core idea. This will entail discontinuous policy evolution, triggered by the technological shift from tangible to intangible content.

Policy concerns around cloud services, in contrast, are likely to evolve not because attention will shift to more fundamental principles, but rather because regular bursts of technological change produce periodic reinterpretation of current principles. Cloud-related policies focus on how to balance the operational and financial benefits of cloud services—primarily raw computing and storage but also networking and applications—against the risk that data will be lost, corrupted, or disclosed. As an article in the January/February 2010 Technology Review put it: “Is the Cloud Safe? It Had Better Be—We All Work There.”

The idea that data-security policy drives technology selection was important long before there were cloud technologies. For example, a subplot in Michael Crichton’s 1996 novel Airframe, which I happened to reread along with the Technology Review article, describes the security/technology compromise under which the Federal Aviation Administration (FAA) trusts and requires aircraft manufacturers to hold the agency’s certification-related technical and forensic data. Certification data are central to the FAA’s work, and holding them at the FAA clearly would streamline the agency’s work. But certification data include proprietary secrets, and having the agency hold them might enable competitors to obtain information through Freedom of Information Act (FOIA) requests. In the novel, the FAA and manufacturers chose to minimize the risk of data exposure through FOIA requests by physically restricting access: keeping data on paper, on dedicated and isolated computers, and on CDs stored only on manufacturers’ premises.

In today’s networked world, the tradeoff between convenience and security unfolds somewhat differently. Data reside and are used within a complex environment that renders physical isolation all but impossible, even within an organization such as an aircraft manufacturer. Encryption therefore replaces isolation as the dominant security mechanism. Translating policy into operations requires cryptographic rather than storage-management or data-center expertise.

Like physical isolation, however, encryption impairs functionality. Although the cloud has evolved differently than the technical challenges of data security, the policy challenge has remained the same: minimizing risk hampers access and therefore degrades functionality. Striking the right balance...
between risk and functionality in the cloud requires policy discussion, and that discussion, in contrast to the discussion surrounding copyright, evolves steadily rather than discontinuously.

Social Networking and Institutional Databases
To affiliate with or be admitted to an online community, participants in social networks such as Facebook disclose personal attributes or views relevant to the community. Most social networkers disclose no more about themselves than is necessary to elicit interesting online engagement within the community, and they then both give and take within the community. The online community, in turn, insulates its members—their disclosures and participation—from outsiders. This is the social compact underlying social networking: disclosure balanced by insulation.

Two closely related policy issues arise when social networking and higher education overlap: (1) whether institutional rules apply to views expressed in or actions conducted in social networks, and (2) whether institutions that become privy to (or seek) social network disclosures or activity can use what they learn for institutional purposes. A peculiar but true story may help frame these issues. A teaching assistant recognized unattributed passages in a graduate student’s paper, tracked down the source, and charged the student with plagiarism. The student conceded that the passages came from a published source, but the student asserted that she had not copied the passages from the published source; rather, she had drawn them from one of her own undergraduate papers written for another institution. The student admitted that the undergraduate paper involved plagiarism. But she argued that there had been no plagiarism by her in graduate school, since reusing one’s own work isn’t plagiarism. In effect, the student was proposing the Vegas principle: what happens in college, stays in college.

Generational divergence will likely ensure that policies are going to evolve continuously in the social networking domain. Today’s younger students tend to value privacy differently than do many older students and staff. Likewise, one might expect, given how often individuals disclose their personal details online, that protection of personal data would be abating as an issue or that students would care about privacy of personal data less than do adults. Yet the trend is precisely the opposite.

For decades, the principal driver for privacy of college and university databases has been the Family Educational Rights and Privacy Act (FERPA). The act requires institutions to specify which student attributes will be publicly available and then to closely restrict access to the rest. Similar requirements have emerged for health information, financial information, and other personal attributes.

But the gradual evolution of data storage from being physically isolated to residing in the cloud has created new opportunities for identity thieves. Their occasional successes have spawned widespread attention to when and how colleges and universities expose personal information. This, in turn, has brought sometimes Draconian requirements for institutions to disclose even benign, accidental data losses, and those disclosures have triggered greater interest and scrutiny. As a result, federal and state requirements governing data protection and exposure have become so complex that full compliance is all but impossible. The fact that each institution interprets the rules independently complicates matters further. The result, in due course, will be fundamental, discontinuous change, with federal legislation likely imposing a uniform set of requirements and, perhaps, more clearly defining liability.

The key point is that how privacy-related policy evolves in social networking differs from how it evolves in institutional database management. The former evolves continuously as technology matures, whereas the latter is likely to evolve discontinuously with the political environment.

Policy Cycles Matter
Policy issues will evolve in many other areas: network neutrality and censorship, the federal role in networking, and collaborative versus commercial application development and support, for example. The EDUCAUSE Review Policy Matters department will track these policy issues, will try to distinguish continuous from discontinuous evolution, and will provide commentary and opinions to help colleges and universities address the federal, state, and institutional policy issues that matter to higher education information technology.

G. A. Jackson ([gjackson@educause.edu]) is Vice President for Policy and Analysis, EDUCAUSE. He serves as Editor of the Policy Matters department for EDUCAUSE Review.

© 2010 G. A. Jackson. The text of this article is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 License (http://creativecommons.org/licenses/by-nc-nd/3.0/).