

Computer Policy and Law

Oh, no . . . not again!" That was the reaction of Cornell University administrators in late 1995. They were reading front-page newspaper articles describing an offensive e-mail message that, signed by four Cornell freshmen, was circulating the Internet and generating protests worldwide. The university officials were remembering the first Internet worm, set loose in 1988 by Robert Morris. Although the origination point of that worm was a computer at MIT, Morris's undergraduate institution, Morris was enrolled as a graduate student in Cornell's Computer Science Department at the time the worm was launched. The burden thus fell on Cornell to investigate and respond.

Part of Cornell's response to the Morris worm was a revised policy on the acceptable use of university computer and network resources, a policy that was developed over several years. The policy was discussed and debated and revised, and discussed and debated some more, before finally being accepted by all campus constituencies. This was the policy in place when the notorious 1995 e-mail started showing up in electronic mailboxes from London to Brisbane.

The policy worked. Notwithstanding the massive publicity surrounding the e-mail message, and despite the mail-bombing and threats, there was no doubt as to process, no need to create policy in the midst of a crisis. The Cornell University judiciary system had clear-cut standards to apply, and when the result was announced and explained, even those who disagreed with the outcome conceded that it had been reached properly.

There's not much more that can be expected of an institutional policy, and Cornell began receiving hundreds of inquiries from campuses that recognized they might easily face a similar situation at any time. Some asked for further information or for permission to use all or part of Cornell's policy; others requested on-site consultations or presentations. It was clear from the volume of these inquiries that there was a large, unmet interest and need throughout higher education for advice and collaboration on institutional technology policies.

It was with this background that, in 1996, Cornell's Office of Information Technologies created the Computer Policy and Law Program, or CPL (<http://www.cornell.edu/cpl/>). The seventh annual CPL Summer Seminar will take place in Ithaca in July 2002, featuring a dozen speakers—lawyers, technologists, and policy experts—and covering topics including copyright, privacy, service-provider liability, and the USA/PATRIOT Act, as well as the basics of the law, technology, and policy-making process. The seminar has expanded from its original two-day format and now runs for three and one-half days. Between sixty and seventy participants will attend from around the country, representing computer-center staff, institutional attorneys, librarians, faculty, judicial-system administrators, security officers, auditors, and a range of other positions.

In addition to its annual seminar, CPL has offered dozens of presentations and workshops on campuses and at conferences since 1996. CPL also runs a Web page featuring a unique and widely respected Internet resource: a database of

links to campus technology policies from nearly eight hundred institutions. These policies are categorized both by type of institution (for example, four-year or two-year, state or private) and by type of policy (for example, e-mail or privacy or acceptable use).

The policy database is part of a reply to one of CPL's most frequently received requests: Can CPL provide a standard policy for another institution to adopt? The answer, since 1996, has been "no," for two general reasons. First, at least as important as the policy itself is the process used to develop the policy. To succeed, a policy must have buy-in: all stakeholders must understand the policy and accept it, an outcome that requires input and participation from the beginning. This can take time—in Cornell's case, as noted, it took years—but short-circuiting the process is almost always a bad idea. When difficult situations arise, as they certainly will, constituencies are more likely to stand behind a policy in which they feel some ownership.

The second reason that CPL rejects one-size-fits-all policies is that one size does *not* fit all. Every institution of higher education is unique. To be effective, technology policies must take into account a wide range of distinctive campus features: the campus culture and climate; the existing judicial system, including expectations for on- and off-campus jurisdiction; whether students live on-campus and, if so, the nature of dormitory networking; requirements of state and local laws, including open-records laws; the institution's charter, including its status as a state or private college; and on and on. Thus the CPL policy database allows

campuses to review and compare a wide variety of policies representing a range of institutions and a range of choices.

Six years ago it would have been reasonable to speculate that by 2002, there would no longer be a need for the Computer Policy and Law Program, since by that time every college and university would likely have established its own, customized technology policy. Perhaps the government would have established clear boundaries for acceptable use of computers and networks, or perhaps the technology itself would have evolved to the point where legal and policy constraints were



built into the systems. Of course, it is clear that we have not outlived our need for campus technology policies in 2002, and from the continuing high level of interest in CPL activities, it is also clear that technology policies remain at best a work-in-progress for many campuses.

Why is it so hard to create technology policies for campuses? There are at least three reasons:

- *The use of computers and networks has increased explosively, both quantitatively and qualitatively.* Students now arrive on campus with computing experience and expectations, not to mention the

computers themselves. Campus policies at variance with that experience and expectations meet resistance. With technology an integral part of student life—from keeping in touch with parents to ordering books from Amazon.com to registering for class and submitting homework—violations of technology policy can no longer be addressed by technology sanctions. On many campuses, losing computer access is equivalent to expulsion. Yet at the same time, with the proliferation of free e-mail services and of wide-area wireless networking, students

will become ever less dependent on campus resources for their Internet connections. Still, regardless of the source of connectivity, incidents of abuse arising from members of a campus community will likely lead to public relations problems for the school and therefore remain a subject for policy.

- *The technology itself keeps changing.* Six years ago, peer-to-peer computing was unknown; Napster was not yet conceived. Multimegabit connections to individual computers were a rarity;

modem-pool policies and etiquette were important topics of discussion. Low-cost, easily configurable wireless access points were not available. Communicating palmtop devices were curiosities, and integrating cell phones with Internet appliances was a venture capitalist's dream. Software to encrypt and decrypt e-mail existed but wasn't sufficiently widespread to be useful. Each of these technology advances raises important policy issues. For example, if staff communicate using encrypted e-mail, what (if any) policy should the campus have for key escrow?

- *The law is not keeping up.* A little more than twenty-five years ago, in 1974, Sony Corporation amazed consumers with an affordable videocassette recorder. Producers of television shows and movies objected, complaining that massive copyright infringement would occur if these new devices caught on. It took ten years for the Supreme Court to finally decide that VCRs were legal. Today's court system does not work any more quickly. Moving from the judicial to the legislative branch, we are faced with an increasing number of new laws governing online privacy, intellectual property, protection of minors, service-provider liability, and commerce; the meaning, the impact, and even the constitutionality of these new laws may not be clear for the foreseeable future. In such an environment, policies must be written carefully and flexibly to avoid the need to make major revisions with each new law and each new court decision.

There seems no end in sight to the need for CPL's work. With this in mind, and in recognition of CPL's past success and future importance, EDUCAUSE has agreed to cosponsor the program with Cornell University. Later this year, the Computer Policy and Law Program will change its name to the EDUCAUSE/Cornell Institute for Computer Policy and Law, or ICPL. A new administrative structure will be put in place for the ICPL, but all current CPL activities will continue, along with some new ones. In particular, the annual seminar in Ithaca will still be held every summer and will still be managed by Cornell. The CPL policy database will remain but will become part of the EDUCAUSE library, benefiting from its support and expertise. In addition, the ICPL will sponsor a variety of workshops and pre-conference seminars linked to existing EDUCAUSE events. Cornell and EDUCAUSE both anticipate a bright—and busy!—future for the new ICPL.

Steve Worona is Director of Policy and Networking Programs at EDUCAUSE. He was a cofounder, with Marjorie Hodges Shaw, of the Cornell Computer Policy and Law Program.