AMERICAN ASSOCIATION OF UNIVERSITY PROFESSORS

This draft report, prepared by a subcommittee of the Association's Committee A on Academic Freedom and Tenure, was approved by Committee A and the AAUP's national Council in November 2013 for publication for comment. We welcome your comments on the draft report; please send them to Jennifer Nichols (jnichols@aaup.org) by January 10.

Academic Freedom and Electronic Communications

In November 2004, the Association's governing Council adopted a report on "Academic Freedom and Electronic Communications," prepared by a subcommittee of Committee A on Academic Freedom and Tenure and approved by Committee A. That report affirmed one "overriding principle":

> Academic freedom, free inquiry, and freedom of expression within the academic community may be limited to no greater extent in electronic format than they are in print, save for the most unusual situation where the very nature of the medium itself might warrant unusual restrictions—and even then only to the extent that such differences demand exceptions or variations. Such obvious differences between old and new media as the vastly greater speed of digital communication, and the far wider audiences that electronic messages may reach, would not, for example, warrant any relaxation of the rigorous precepts of academic freedom.

This fundamental principle still applies, but developments since the publication of the 2004 report suggest that a fresh review of issues raised by the continuing growth and transformation of electronic communications technologies and by the evolution of law in this area is appropriate. For instance, the 2004 report focused largely on issues associated with e-mail and the posting of materials on websites, online bulletin boards, learning management systems, blogs, and listservs. Since then new social media, such as Facebook, LinkedIn, Reddit, Tumblr, and Twitter, have emerged as important vehicles for electronic communication in the academy.

Already in 2004 it was clear that electronic communications could easily be forwarded to others at vastly greater speeds, with potentially profound implications for both privacy and free expression. As Robert M. O'Neil has written,

> An electronic message may instantly reach readers across the country and indeed around the globe, in sharp contrast to any form of print communication. Although a digital message, once posted, can be infinitely altered over time—another significant difference—the initial message may never be retracted once it has been sent or posted. Indeed, the first posting

> may remain accessible on 'mirror' sites despite all efforts to suppress, remove, and expunge it.[1]

Electronic communications can be altered, or presented selectively, such that they are decontextualized and take on implicit meanings different from their authors' original intent. With the advent of social media such concerns about the widespread circulation and compromised integrity of communications that in print might have been essentially private have only multiplied further.

Moreover, while the 2004 report assumed that electronic communications generated by faculty in the course of their teaching and research were physically located on servers and computers owned and operated by their colleges and universities, today institutions increasingly employ technologies associated with cloud computing and other outsourcing strategies. These may involve relinquishing control to third-party services, storing data at multiple sites administered by several organizations, and relying on multiple services to operate across the network—a shift that may pose potentially profound challenges to academic freedom.

These changes have been magnified by the growing proliferation of new electronic communications devices, such as smartphones and tablets. At Oakland University in Michigan, for example, the university's roughly 7,500 students now bring an average of 2.5 devices each to campus, while faculty members bring on average two.[2] The desire on the part of increasing numbers of faculty, staff, and students to have access to communications and information on multiple devices, especially mobile devices, has increasingly driven institutions to create "BYOD" (bring-your-own-device) policies. By embracing individual consumer devices (BYOD), an institution may better address the personal preferences of its faculty, staff, and students, offering not only increased mobility but also increased integration of their personal, work, and study lives. However, the increasing number of devices and the increasing demand for bandwidth from new applications have begun to strain institutional resources in ways that may lead institutions to seek access restrictions that could adversely affect academic freedom.

More important, such practices can further blur already problematic boundaries between communications activities that are primarily extramural or personal and those that are related more directly to teaching and scholarship. Digital devices such as smartphones have also promoted increased interactivity between users and their devices, permitting users to create their own content but also to leave personal "footprints," which may be subject to surveillance.

As in 2004, "college and university policies that were developed for print and telephonic communications"—and policies developed for earlier modes of electronic communications—"may simply not fit (or may fit imperfectly) the new environment." **Faculty need to understand more completely the implications for academic freedom of the expanded use and variety of electronic communications technologies, and they should be directly involved in the formulation and implementation of policies governing such technology usage.**

---

[1] Robert M. O'Neil, *Academic Freedom in the Wired World* (Cambridge: Harvard University Press, 2008), pp. 179–80.

[2] Carl Straumsheim, "Device Explosion," *Inside Higher Ed*,September 5, 2013, http://www.insidehighered.com/news/2013/09/05/wireless-devices-weigh-down-campus-networks.

1. Freedom of Research and Publication

The 2004 report affirmed: "The basic precept in the 1940 *Statement of Principles on Academic Freedom and Tenure* that 'teachers are entitled to full freedom in research and in the publication of the results' applies with no less force to the use of electronic media for the conduct of research and the dissemination of findings and results than it applies to the use of more traditional media." As that report noted, however, access to materials in digital format may be subject to greater restrictions than would be the case with print-format materials.

Access to Information in Digital Format

Academic freedom is dependent on a researcher's ability not only to gain access to information but also to explore ideas and knowledge without fear of surveillance or interference. Historically, scholars have gained access to published and often to unpublished research materials through college and university libraries. Increasingly nowadays, electronic communications technologies permit libraries to offer access to a far broader array of materials than in the past, through a wide variety of online databases. Some online catalogs, designed to replicate social media, now allow users to leave notations and reviews of catalogued materials that can be viewed around the world.

To be sure, as Robert M. O'Neil has noted, "[a]lthough a university does to some degree control a scholar's recourse to print materials by its management of library collections, . . . the potential for limitation or denial of access is vastly greater when the institution maintains and therefore controls the gateway to the Internet."[3] Colleges and universities certainly are entitled to restrict access to their library resources, including electronic resources, to faculty, students, staff, and other authorized users, including alumni and recognized scholars from other institutions, in accordance with policies adopted by the institution with the participation of faculty. But the extent to which access to electronic materials may be limited is not always under the control of the library or even of the institution. Third-party vendors may seek to impose restrictions on access that go beyond those claimed by the institution itself, and such restrictions are rarely defined by faculty governance structures. Those vendors may also impose auditing requirements that are conflict with librarians' duties to respect and protect the confidentiality of patrons.

Concerns about access were heightened in early 2013 following the tragic suicide of open-access advocate Aaron Swartz. In 2011, a federal grand jury had indicted Swartz for the alleged theft of millions of journal articles through the JSTOR account of the Massachusetts Institute of Technology (MIT). Swartz reportedly wanted to make all of those articles freely available. Authorities charged that he had used an MIT guest account, even though he did not have a legal right to do so. At the time of his death Swartz faced the prospect of millions of dollars in fines and legal costs and decades in prison, if he had been convicted. Despite reports that he had suffered from depression, most observers believe that his legal troubles led to his suicide.

[3] O'Neil, p. 181.

Although JSTOR declined to pursue action against Swartz, some charged that "MIT refused to stand up for Aaron and its own community's most cherished principles."[4] Ironically, however, it was MIT's relatively open policy of access to its network that had enabled Swartz to obtain the downloaded materials. MIT's own subsequent investigation of the matter acknowledged that the institution had missed an opportunity to emerge as a leader in the national discussion on law and the Internet. But the university denied any active role in his prosecution.[5]

Scholars have also debated whether Swartz's action could even be regarded as a kind of theft, as some had charged. "The 'property' Aaron had 'stolen,' we were told, was worth 'millions of dollars,'" wrote Harvard law professor Lawrence Lessig, "with the hint, and then the suggestion, that his aim must have been to profit from his crime. But anyone who says that there is money to be made in a stash of academic articles is either an idiot or a liar."[6]

The complicated copyright and other issues raised by the open-access movement are beyond the scope of this report. While the expanding digital world has promised to make information freely accessible to a global community, commercial forces have locked up most research behind paywalls and ever-more-restrictive licensing agreements. Faculty members who produce research in digital form frequently do not control how that research may be accessed and by whom. The AAUP's 1999 *Statement on Copyright*[7] affirmed that "it has been the prevailing academic practice to treat the faculty member as the copyright owner of works that are created independently and at the faculty member's own initiative for traditional academic purposes." Any consideration of open access must start from this principle.[8]

Often college and university libraries are themselves compelled to accede to the demands of outside vendors. Libraries and librarians can, however, promote open access to information by supporting institutional repositories, hosting open-access journals, and working with faculty to promote the value of more open modes of scholarly communication. Libraries can also collaborate with others

---

[4] Scott Jaschik, "Academe reacts to Aaron Swartz's suicide," *Inside Higher* Ed, January 14, 2013, http://www.insidehighered.com/news/2013/07/31/mit-releases-report-its-role-case-against-internet-activist-aaron-swartz.

[5] Colleen Flaherty, "Could Have Done More," *Inside Higher Ed,* July 31, 2013, http://www.insidehighered.com/news/2013/07/31/mit-releases-report-its-role-case-against-internet-activist-aaron-swartz.

[6] Ibid.

[7] AAUP, *Policy Documents and Reports*, 10th ed. (Washington, DC: AAUP, 2006), 214-216.

[8] As of August 2013, more than 175 universities had endorsed open access. That month, for instance, the University of California's Academic Senate adopted an open-access policy that will make research articles freely available to the public through eScholarship, California's open digital repository. The policy applies to all ten of the system's campuses with more than 8,000 tenured and tenure-track faculty members and will affect as many as 40,000 research papers a year. Faculty members can opt out or ask that their work be embargoed for a period of time, as many journal publishers require. In a departure from many other institutions' open-access policies, UC researchers will also be able to make their work available under commercial as well as noncommercial Creative Commons licenses. UC researchers get an estimated 8 percent of all U.S. research money and produce 2 percent to 3 percent of peer-reviewed scholarly articles published worldwide every year. See "Open Access Gains Major Support in U. of California's Systemwide Move," *Chronicle of Higher Education*, August 5, 2013.

or work independently to develop a role as publisher both for new content and through digitization of material that is in the public domain or otherwise lawfully available for digitization.[9]

When resources are provided by third-party vendors, the library may also lose control over privacy and confidentiality. When a faculty member visits the library to read a book or journal article, this activity takes place without triggering any issues related to recordkeeping or permissions. In the electronic journal and e-book environment, however, records of access and permissions may be critical to resolving issues about licensing and copyright infringement, and the existence of these records may compromise user confidentiality. Sometimes the identity of a person reading a resource is even embedded—both electronically and in text—in the journal article. Such features may violate state laws protecting the confidentiality of library circulation records.

The commitment of libraries and librarians to maximizing access to information and protecting user privacy and confidentiality should not change in the face of new technologies. The maintenance of usage logs for licensing reasons, for diagnosing technical problems, or for monitoring computer performance may be necessary, but libraries must strive to minimize such monitoring and to compile information as much as possible only in the aggregate. Thus, for example, when the library identifies a user as authorized to gain access to a journal held by another entity, it should indicate only that the user is affiliated with the institution without sharing that user's identity.

Nevertheless, third-party vendors may gain access to user information, especially when these vendors offer research tools such as customized portals, saved searches, or e-mail alerts on research topics. How these vendors employ such information and who can gain access to it may be beyond the library's control. Librarians thus have a responsibility to educate users about the potential dangers of using third-party tools.

Faculty members can also play a role in shaping the policies of publishers and online vendors regarding access to published research and monitoring of individual users through their roles as members of editorial boards and holders of managerial positions in academic societies and with private publishers. Faculty members in these positions can work with academic libraries to collaborate on developing cost-effective business models that encourage broad and confidential access to publications. **College and university libraries need to review existing policies on privacy and confidentiality to ensure that they have kept pace with practices and technologies in the library.[10] In addition, when negotiating contracts with vendors, librarians should require those vendors to protect user information to the same degree as if it were in the custody of the library.** And, building on the success of laws in forty-eight states that protect the confidentiality of library users, as well as provisions of the Family Educational Rights and Privacy Act that protect the privacy of educational records, colleges and universities should advocate additional legislation that would provide the same level of protection to information held by third parties on behalf of libraries and their users, whether it is library-controlled information hosted on a server in another state, cloud-hosted information, or user-supplied information in a vendor's customizable portal.

---

[9] One example of such a collaboration may be found at http://www.philosophersimprint.org/, an open-access online resource for philosophy scholarship, whose mission is "to overcome [the] obstacles to the free electronic dissemination of scholarship."

[10] For more on library privacy and confidentiality policies, see the following site maintained by the American Library Association: http://www.ala.org/offices/oif/ifissues/privacyconfidentiality.

The 2004 report noted that "[i]n many disciplines, scholars may quite legitimately share material that would be deemed 'sexually explicit'—art, anatomy, psychology, etc. Such sharing is at least as likely to occur electronically as it has traditionally occurred in print. The difference in medium should no more affect the validity of such exchanges than it should justify a double standard elsewhere." AAUP policy elsewhere recognizes that academic freedom encompasses freedom of artistic expression "in visual and performing arts."[11] Increasingly, artistic expression that challenges conventional tastes and norms involves digital images, even more than images on canvas or film. It is thus vital to affirm that academic freedom applies to such modes of artistic expression and the need for its protection is not limited to traditional media. At the same time, the 2004 policy on electronic communications acknowledged that there may "be legitimate institutional interests in restricting the range of persons eligible to receive and gain access to such material—especially to ensure that minors are not targeted."

Although in 1968 the U.S. Supreme Court recognized that material that is not legally obscene but is "harmful to minors" may be regulated,[12] subsequent rulings have severely limited the application of this principle when it might affect access to such material by adults.[13] In this light, **institutional policy should make clear that faculty in the course of their research have the right to access and circulate electronically all legal materials, no matter how controversial and even if these might be considered "harmful to minors."**

In particular, colleges and universities should refrain from employment of so-called "filtering" software that limits access to purportedly "harmful" or even "controversial" materials. It is questionable whether such filters are appropriate or effective in school and public libraries, but they surely have no place in higher education facilities. Filters are especially insidious because users often cannot know whether and, if so, why they have been denied access to a site or resource.

Security Versus Access

In recent years, many university information technology systems have come under sustained cyberattack, often from overseas. While these attacks have sometimes resulted in the theft of personal information, such as employee social security numbers, faculty research materials have been a frequent target. A particularly inviting target is patentable research, some with vast potential value, in areas as disparate as prescription drugs, computer chips, fuel cells, and aircraft and medical devices. Institutions' infrastructure more generally has also been under threat. Some universities have experienced as many as 100,000 hacking attempts each day.[14]

---

[11] AAUP, *Policy Documents and Reports*, 10th ed. (Washington, DC: AAUP, 2006), 35-36.

[12] *Ginsberg v. New York*, 390 U.S. 629 (1968).

[13] In 1997, the Court struck down the Communications Decency Act, and in 2009, it declined to review a decision by the U.S. Court of Appeals for the Third Circuit striking down the Children's Online Protection Act. *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997) and *ACLU v. Mukasey*, 534 F.3d 181 (3rd Cir. 2008), cert. denied, 555 U.S. 1137 (2009).

[14] Richard Pérez-Peña, "Universities Face a Rising Barrage of Cyberattacks," *New York Times*, July 16, 2013, http://www.nytimes.com/2013/07/17/education/barrage-of-cyberattacks-challenges-campus-culture.html?_r=0.

The increased threat of hacking has forced many universities to rethink the basic structure of their computer networks. "A university environment is very different from a corporation or a government agency, because of the kind of openness and free flow of information you're trying to promote," said David J. Shaw, the chief information security officer at Purdue University. "The researchers want to collaborate with others, inside and outside the university, and to share their discoveries."[15]

While many corporate sites restrict resources to employees, university systems tend to be more open, and properly so. The most sensitive data can be housed in the equivalent of small vaults that are more difficult to access and harder to navigate, use sophisticated data encryption, and sometimes are not even connected to the larger campus network, particularly when the work involves dangerous pathogens or research that could turn into weapons systems.

Some universities no longer allow their professors to take university-owned or -leased laptops to certain foreign countries. In some countries the minute one connects to a network, information on one's computer will be copied, or remote devices like computer cookies or malware that enable undetected transferal of information to a home network will be planted in the computer. Many institutions have become stricter about urging faculty to follow federal rules that prohibit taking some kinds of sensitive data out of the country or have imposed their own restrictions, even tighter than the government's. Still others require that employees returning from abroad have their computers scrubbed by professionals before they may access university servers.

These are genuine concerns, and universities are well advised to devote resources to protecting their electronic communications networks. However, every effort should also be made to balance the need for security with the fundamental principles of open scholarly communication.

Scholarly Communication and Social Media

The advent of social media has raised some new questions about how scholars communicate about their research. For example, professors who present papers at scholarly conferences often use those occasions to try out new ideas and stimulate discussion. While they may be willing, even eager, to share preliminary ideas with a closed group of peers, they may be less happy to have those in attendance broadcast these ideas via social media. Conference papers are often clearly labeled as "not for circulation." At some meetings, however, attendees at sessions have communicated to others electronically—and often instantaneously—via social media, e-mails, or blog posts, reports and comments on papers and statements made by other conference presenters and attendees.[16]

Many academic conferences and sometimes individual conference sessions have specific Twitter hash tags associated with them—at times suggested by the conference organizers. As a result, ideas and information that previously would have been controlled by the presenter and limited to a relatively small audience may quickly become accessible globally. Some have worried that reports on social media of conference proceedings might increase the likelihood that others could pirate or exploit a presenter's new and original ideas before that individual has an opportunity to develop them. While this concern may be exaggerated, it is clear that new forms of social media and

[15] Ibid.

[16] Steve Kolowich, "Scholars debate etiquette of live-tweeting academic conferences," *Inside Higher Ed*, October 2, 2012, http://www.insidehighered.com/news/2012/10/02/scholars-debate-etiquette-live-tweeting-academic-conferences.

electronic communications technologies can make research in progress both more accessible and more vulnerable to intellectual property theft. In effect, anyone with an Internet connection can function as a reporter publishing accounts of others' work.

"The debate over live tweeting at conferences is, in many ways, about control and access: who controls conference space, presentation content, or access to knowledge?" wrote one doctoral student. A professor responded with objections to sharing "other people's work without asking." For some the debate is generational. "I see this as a divide between older and newer forms of academic culture," wrote one younger scholar. "On the traditional model, you don't put an idea out there until it's fully formed and perfect."[17]

Of course, scholars have always debated each other's ideas and will continue to do so. However, **faculty members who use social media to discuss research should keep in mind the intellectual property rights of their colleagues as well as their own academic freedom to comment on and debate new ideas.**

2. Freedom of Teaching

According to the 1940 *Statement of Principles on Academic Freedom and Tenure*, "teachers are entitled to freedom in the classroom in discussing their subject." But what constitutes a classroom? The 2004 statement noted that "the concept of 'classroom' must be broadened" to reflect how instruction increasingly occurs via a "medium that clearly has no physical boundaries" and that "[t]he 'classroom' must indeed encompass all sites where learning occurs."

If anything, the boundaries of the "classroom" have only expanded in the past decade. It is now more common than not for even the most traditional "face-to-face" classes to include material offered via online learning management systems. And the rapid development and perhaps over-hyped promise of totally online education, including the explosive growth of Massive Open Online Courses (MOOCs), frequently offered by for-profit private corporations, suggests that academic freedom in the online classroom is no less critical than it is in the traditional classroom.

This report is not the place to discuss all the myriad issues of academic freedom, shared governance, intellectual property, and institutional finances raised by the spread of online education. However, it is critical to reiterate that **a classroom is not simply a physical space, but any location, real or virtual, in which instruction occurs, and that in classrooms of all types the protections of academic freedom and of the faculty's rights to intellectual property in lectures, syllabi, exams, and similar materials are as applicable as they have been in the physical classroom.**

In August 2013, the teaching duties of a tenured Michigan State University professor were reassigned after a student anonymously videotaped part of a 90-minute lecture, a heavily edited two-minute version of which—described by some as an "anti-Republican rant"—was then aired on a conservative Internet site, on Fox News, and on YouTube, where it was viewed more than 150,000 times. In October 2013, a geography professor at the University of Wisconsin--La Crosse sent her students an e-mail explaining that they could not access census data to complete a required assignment because the "Republican/Tea Party-controlled House of Representatives" had shut

[17] Ibid.

down the government, which closed the U.S. Census Bureau's website. After a student posted the e-mail on Twitter, it appeared in a local newspaper and in national conservative media, resulting in numerous complaints to the university administration, which sent an e-mail to the campus distancing the institution from the comment.[18]

These and similar incidents demonstrate that electronic media can expand the boundaries of the classroom in new and dramatic ways. And while classroom lectures, syllabi, and even instructors' e-mail to students should be considered the intellectual property of the instructor, much of what teachers distribute to students in the classroom or write in e-mails may legally be redistributed by students for noncommercial uses under the "fair use" principle. Moreover, copyright does not cover expression that is not reduced to "tangible" form, including extemporaneous utterances such as those of the Michigan professor, as it might in the case of written materials like a syllabus or formal lectures and PowerPoint presentations.

Surreptitious recording of classroom speech and activity may exert a chilling effect on the academic freedom of both professors and students.[19] Faculty should also be aware that electronic communications with students can easily be recirculated without the permission of either party.

It should be further noted that new teaching technologies and learning management systems also allow faculty members and students to be monitored in new ways. Online teaching platforms and learning management systems may permit faculty members to learn whether students in a class did their work and how long they spent on certain assignments. Conversely, however, a college or university administration could use these systems to determine whether faculty members were logging into the service "enough," spending "adequate" time on certain activities, and the like. Such monitoring should not be permitted without the explicit and voluntary permission of the instructor involved.

While learning management systems make it possible for faculty to keep electronic teaching materials separate from scholarly, political, or personal material often found on faculty websites, many instructors still frequently post course materials on websites alongside other content, some of which may be controversial. Students who encounter material they find disturbing while accessing a faculty website in search of course materials may complain to the administration or even to the courts. While all legal material on faculty websites should enjoy the protections of academic freedom, instructors should exercise care when posting material for courses on sites that also include potentially controversial noninstructional materials.

---

[18] Colleen Flaherty, "Not-so-great expectations," *Inside Higher Ed*, October 18, 2013, http://www.insidehighered.com/news/2013/10/18/professors-afforded-few-guarantees-privacy-internet-age.

[19] The AAUP has been concerned with this issue since its 1915 *Declaration of Principles on Academic Freedom and Academic Tenure*, which stated: "Discussions in the classroom ought not to be supposed to be utterances for the public at large. They are often designed to provoke opposition or arouse debate." In the 1980s a group called "Accuracy in Academia" encouraged students to record professors' classroom statements and send them to the organization to be tested for "accuracy." In a 1985 statement issued jointly with twelve other higher-education associations, the AAUP asserted, "The classroom is a place of learning where the professor serves as intellectual guide, and all are encouraged to seek and express the truth as they see it. The presence in the classroom of monitors for an outside organization will have a chilling effect on the academic freedom of both students and faculty members. Students may be discouraged from testing their ideas, and professors may hesitate before presenting new or possibly controversial theories that would stimulate robust intellectual discussion."

3. Access to Electronic Communications Technologies

Colleges and universities commonly adopt formal electronic communications policies, which define access to the institution's electronic communications network and, through that network, to the Internet. Such policies generally try to balance the need, on the one hand, to protect the university's electronic resources from outside hacking and to safeguard confidential personal and research information and, on the other hand, to provide free access to authorized users. **Although security and liability concerns may result in legitimate constraints being placed on usage, in general no conditions or restrictions should be imposed upon access to and use of electronic communications technologies more stringent than limits that have been deemed acceptable for the use of traditional campus channels of communication.**

An institution may, for example, acceptably require each faculty user to obtain and enter a password and to change that password periodically. The university also has an interest in protecting its faculty, staff, and students from spam and in limiting how much bandwidth an individual may use so as to ensure that computing resources are not overburdened or squandered. However, wholesale bans on streaming video may constitute a violation of academic freedom. Some institutions have limited access to streaming video and audio in student dormitories to avoid both illegal downloading of copyrighted material and overburdening the network. But such restrictions should not be automatically extended to faculty, who may need access to such sites in order to obtain materials for teaching or research. Moreover, restrictions that deny use for "personal matters" or limit usage to "official university business" can reduce productivity and are both unnecessary and problematic, as many private businesses have learned.

In an often well-intentioned effort to reduce spam and prevent the monopolization of bandwidth, some university information technology offices have proposed policies under which users of institutional electronic communications resources must seek advance permission to send messages to large groups of recipients. But even if such measures address the problems of spam and limited bandwidth—and it is questionable whether they do—they only create a much larger and more ominous academic freedom problem because they amount to de facto prior censorship. Similarly, provisions that have been proposed in some instances to bar communications that purportedly "interfere with the mission of the university" or that violate university policies also lead to unwarranted censorship of free expression.

Some states have also barred public employees, including university faculty at public institutions, from employing the institution's electronic communications resources—for example, a university e-mail account—for political campaigning. In such states, public colleges and universities must clearly define what constitutes such activity. While a public employee may reasonably be barred, for instance, from using a university website to run for public office or raise funds for a political campaign, policies that discourage or prohibit faculty, staff, and students from expressing political preferences clearly violate fundamental principles of free expression.

Electronic resources should also be made available equally to all employees, including faculty, for the purposes of union or other organizing activity. While the National Labor Relations Board has ruled that private employers may bar employees from using employer-owned e-mail accounts for non-work-related communications, if those employers do permit such activity they may not discriminate against union-related e-mail use nor can they bar the use of social media for discussion of working

conditions.[20] **The AAUP has upheld the right of faculty members to speak freely about internal university affairs as a fundamental principle of academic freedom that applies as much to electronic communications as it does to written and oral communications. This includes the right of faculty members to communicate with one another about their conditions of employment and to organize on their own behalf.**

Frequently university policies attempt to delineate user "rights" and "responsibilities," but too often those policies emphasize only the latter. Administrations at some institutions appear to view computer and Internet access as a lower-order faculty perquisite that they may summarily terminate. Such views need to be rejected unequivocally. Access to campus computing facilities, and through them to the Internet, represents a vital component of faculty status for most scholars and teachers, especially as cost-cutting measures have caused libraries to rely more heavily on electronic instead of print journals. While it would be naïve to suggest that circumstances might never warrant the withdrawal or suspension of digital access, such access may be denied or limited only for the most serious of reasons (e.g., creating and unleashing a destructive virus), and only after the filing of formal charges and compliance with rigorous disciplinary procedures that guarantee the protections of academic due process to the accused individual, even where the transgression may not be so grave as to warrant dismissal or suspension.

A university's policies must specify the infractions that might warrant such a sanction, recognizing only conduct that jeopardizes the system and the access of others. The policy should also prescribe the procedures to be followed in such a case. In exigent circumstances, a faculty member's computer access might be summarily and briefly suspended during an investigation of serious charges of abuse or misuse. Any such suspension should, however, be no longer than necessary to conduct the investigation, and should be subject to prior internal faculty review.[21]

Indeed, **any restrictions that an institution may seek to impose on a faculty member's access and usage must be narrowly defined, and clearly and precisely stated in writing.** In addition, institutions should include in their electronic communications policy a statement similar to that found in the University of California policy: "In general, the University cannot and does not wish to be the arbiter of the contents of electronic communications. Neither can the University always protect users from receiving electronic messages they might find offensive."[22]

4. Outsourcing of Information Technology Resources

Many campuses have considered outsourcing the provision of non-instructional information technology (IT) resources, such as e-mail servers, calendaring, and document storage. Outsourcing to a technology company can provide advantages to institutions, such as lower cost and potentially better security, and help an institution focus on its core mission of education instead of on the

---

[20] The Guard Publishing Company, d/b/a *The Register Guard*, 351 NLRB 1110 (2007), supplemental decision, 357 NLRB No. 27 (2011); Hispanics United of Buffalo, Inc., 359 NLRB No. 37 (2012).

[21] AAUP-recommended procedures for the imposition of sanctions may be found in *Recommended Institutional Regulations on Academic Freedom and Tenure*, Regulation 7, at http://aaup.org/report/recommended-institutional-regulations-academic-freedom-and-tenure.

[22] University of California Electronic Communications Policy: http://www.ucop.edu/ucophome/policies/ec/html/pp081805ecp.html#PROVISIONS.

provision of services.[23] Prior to the cloud outsourcing model, institutions operated in-house technical resources, and the information generated by their use remained physically within the walls of the institution. However, in many cloud models it is assumed, sometimes without explicitly stating, that the outside service provider can analyze how these resources are used for the provider's own benefit. Thus cloud services proceed from a fundamentally different set of assumptions from those that govern the same services provided in-house at institutions.

Faculty and student communications are important and can be unusually vulnerable to a variety of threats. Communications may contain a variety of private or confidential information concerning the development of new drugs, classified research, export-controlled research, and advice to clients visiting institutionally operated legal clinics. Electronic communications may be targets of government surveillance. Institutions also have special duties, including legal and ethical obligations to protect information about students.

Outsourcing presents several identifiable risks. For instance, outside providers may be motivated to offer services that they can develop and serve "at scale" and that do not require special protocols. These services may have been designed for businesses, and thus the services themselves may not be tailored for the special context of higher education or for the roles that faculty members play in colleges and universities. In effect, outsourcing may undermine governance, as the provider may effectively set and change policy without consulting campus "IT" leadership or faculty.[24]

Several approaches could strengthen an institution's commitment to academic freedom even in outsourced situations:

1. The institution should formally involve faculty in decisions to outsource core electronic communications technologies.

2. The process of selecting an outside provider selection must involve the consideration of factors other than price, including institutional needs, legal and ethical obligations, and the norms and mission of the institution.

3. IT leadership should carefully evaluate the outside provider's ability to access content and electronic traffic data. It is important to note that even if a provider promises not to provide usage data to advertisers, that promise does not foreclose analysis of electronic communications data for other purposes, including commercial purposes. An agreement should be reached in advance with the outside provider to prohibit the sharing of such data with commercial interests.

4. Faculty should encourage campus IT leadership to collaborate with other institutions in jointly identifying problems and mitigating risks.

5. IT leadership should carefully evaluate the outside provider's uses, processing, and analysis of user content and transactional data. All uses of data should be reviewed by the institution and specifically authorized.

---

[23] Outsourcing of instruction through online education offered by outside providers, however, is a quite different matter.

[24] The abbreviation "IT" is used here and subsequently in reference to those university offices and functions variously called "information technology," "instructional technology," or "institutional technology."

6. IT leadership should follow policy decisions and changes of outsource providers, and notify faculty when these decisions implicate governance issues.

7. IT leadership should consider technical approaches to reduce lock-in to outside providers and, where possible, to mask content and traffic data from these providers.

8. Contracts with outside vendors of electronic communications services should explicitly reflect and be consistent with internal institutional policies regarding such communications and with applicable federal and state laws.

5. Unwarranted Inference of Speaking for or Representing the Institution

The 1940 *Statement of Principles* cautions that faculty members "should make every effort to indicate that they are not speaking for the institution" when in fact they are not doing so. The meaning of that constraint is clear enough in the print world. One may refer to one's faculty position and institution "for identification purposes only" in ways that create no tenable inference of institutional attribution. In the digital world, however, avoiding an inappropriate or unwarranted inference may be more difficult.

The very nature of the Internet causes attribution to be decontextualized. A statement made by a faculty member on a website, in an e-mail, or in a communication via social media communication might be recirculated broadly, and any declaration that the institution bears no responsibility for the statement will be lost. What about statements made on Twitter, which limits communications to 140 characters? It is hardly reasonable to expect a faculty member to indicate on every tweet that she or he is not speaking for the institution. And Facebook pages have a fixed template that does not allow for a banner disclaimer in a readily visible spot on an individual's main page.

In late 2012, a professor at Florida Atlantic University posted on his blog a controversial statement expressing skepticism about official accounts of the murder of students at Sandy Hook Elementary School in Connecticut that year. The blog included this statement: "All items published herein represent the views of [the professor] and are not representative of or condoned by [the university]." Yet the university claimed that even by mentioning his affiliation the professor had failed to distinguish his personal views from those of the university adequately and thereby damaged the university. As a result, he was issued a formal reprimand.[25] In a letter to the university president, the AAUP staff wrote that the professor

> may indeed have posted highly controversial statements on his website; but it is such speech, in particular, that requires the protection of academic freedom. . . . In our time, when the Internet has become an increasingly important vehicle for free intellectual and political discourse around the world, the [university] administration's action, if allowed to stand, sets a precedent that potentially chills the spirited exchange of ideas—however unpopular, offensive, or controversial—that the academic community has a special responsibility to protect.

[25] Scott Jaschik, "Reprimand for a Blog," *Inside Higher Ed*, April 12, 2013, http://www.insidehighered.com/news/2013/04/12/florida-atlantic-reprimands-professor-over-his-blog.

Institutions may reasonably take steps to avoid inferences of institutional attribution or agreement, in ways that print communications might not warrant. Disclaimers may be useful, though their value is often exaggerated. However, the nature of electronic communication itself tends to decontextualize meaning and attribution, and **faculty members cannot be held responsible for always indicating that they are speaking as individuals and not in the name of their institution, especially if doing so will place an undue burden on the faculty member's ability to express views in electronic media.**

6. Social Media

The 2004 report essentially assumed that electronic communications were either personal (if not wholly private), as with e-mail, or public (or open access), as with websites, blogs, or faculty home pages. The growth of social media calls such an assumption into question. Social media sites blur the distinction between private and public communications in new ways. Unlike blogs or websites, which are generally accessible to anyone with Internet access who goes in search of the site, social-media sites offer the appearance of a space that is simultaneously private and public, one that is on a public medium (the Internet) and yet defined by the user through invitation-only entry points, such as Facebook "friend" requests, and a range of user-controlled privacy settings.

The extent of the privacy of such sites, however, is at the least uncertain and limited, because it is dependent not only on the individual's privacy-setting choices and those of the members in the individual's network, but also upon the service providers' practices of analyzing data posted on the network. Moreover, social-media providers often modify their policies on privacy and access in ways that their users do not always fully comprehend. Faculty members may believe that their Facebook pages are more secure or private than a personal web page, but that is not necessarily true. The seemingly private nature of sites like Facebook, Flickr, or Pinterest can lead individuals to let down their guard more readily, because they may think they are communicating only to handpicked friends and family, when in fact those friends and family may be sharing their utterances with other unintended recipients without the individual's knowledge.[26] These sites are not closed portals, despite what their account controls may suggest. Likewise, an acquaintance may post private information about a faculty member's personal life without that faculty member's knowledge (or vice versa), and the viral nature of social-media sites may then make that comment more public than the original poster intended.

Evidence abounds that such concerns are not unwarranted. One prominent example was the 2010 case of a professor at East Stroudsburg University in Pennsylvania who was suspended from her faculty position and escorted off campus by police after a student reported one of her Facebook status updates ("Had a good day today. Didn't want to kill even one student.") to the administration. The professor alleged that she did not know that anyone other than her personal Facebook network could gain access to her status updates.

In another example, also from 2010, the administration at a theological seminary summarily dismissed an assistant professor of church history and languages who was also library director,

[26] Social-media communications may also be used by the social-media site itself for data-mining purposes.

allegedly because of a comment he had posted on a former student's Facebook page a month earlier, predicting that "one day the Catholic Church will . . . approve of openly gay priests." In June 2013, an evolutionary psychology professor sparked an uproar after he told his Twitter followers that overweight students are not cut out for PhD programs. The professor quickly deleted the tweet, but he faced considerable criticism, especially after he tried to justify his comment by claiming it was part of a research project. The administration disciplined him for what he had written.[27]

In September 2013, the administration of Johns Hopkins University asked a tenured professor, a prominent authority on Internet security and privacy issues, to remove a blog post, claiming that the post contained a link to classified information and used the logo of the National Security Agency (NSA) without authorization. The post was about NSA privacy debates and encryption engineering. The university has numerous ties with the NSA. The administration withdrew the request after the professor discussed it on Twitter and in the media.[28]

At the University of Kansas, also in September 2013, a journalism professor, responding to a shooting incident at the Washington Navy Yard in Washington, DC, tweeted a comment about gun control that many gun advocates found offensive. He was barraged with hate messages and death threats, and several legislators called for his dismissal. Although the university publicly reaffirmed its commitment to his freedom of speech, he was suspended to "avoid disruption." However, a suspension designed to protect a faculty member from potentially violent responses to a controversial statement can quite easily become a punishment for the content of the statement, which in this instance was clearly protected by both the First Amendment and principles of academic freedom.[29]

Many faculty members have decided that they will simply not join Facebook or similar sites. Others have decided that it would be improper ever to connect with a student on a social network. Most colleges and universities have yet to formulate policies regarding social-media usage by faculty. At institutions where such policies exist, the focus is frequently on the university's reputation and not on the faculty's academic freedom. So, for instance, the University of South Carolina Upstate's "Social Media Policy and Procedure Guidelines" includes the following: "The purpose of the Social Media Policy is to ensure accuracy, consistency, integrity, and protection of the identity and image of the University of South Carolina Upstate by providing a set of required standards for social media content from any department, school, facility, organization, entity, or affiliate."[30] It is unclear whether or to what extent this policy applies to individual faculty members.

This report recommends that each institution work with its faculty to develop policies governing the use of social media. Any such policy must recognize that social media can be used to make extramural utterances, which are protected under principles of academic freedom. As Committee A previously noted regarding extramural utterances, "Professors should . . .

---

[27] Lauren Ingeno, "#Penalty," *Inside Higher Ed*, August 7, 2013, http://www.insidehighered.com/news/2013/08/07/fat-shaming-professor-faces-censure-university.

[28] "Hopkins (Briefly) Asks Professor to Remove Blog Post" *Inside Higher Ed*, September 10, 2013, http://www.insidehighered.com/quicktakes/2013/09/10/hopkins-briefly-asks-professor-remove-blog-post.

[29] Scott Rothschild and Ben Unglesbee, "Professor getting death threats over NRA tweet, colleagues support his free-speech rights," *Lawrence Journal-World*, September 23, 2013, http://www2.ljworld.com/news/2013/sep/23/firestorm-over-guths-comment-continues-university-/.

[30] https://www.uscupstate.edu/uploadedFiles/Offices/Communications/social/Social%20Media%20Policy%20Approved.pdf.

have the freedom to address the larger community with regard to any matter of social, political, economic, or other interest, without institutional discipline or restraint, save in response to fundamental violations of professional ethics or statements that suggest disciplinary incompetence."[31] Obviously, the literal distinction between "extramural" and "intramural" speech—speech outside or inside the university's walls—has little meaning in the world of cyberspace. But the fundamental meaning of extramural speech, as a shorthand for speech in the public sphere and not in one's area of academic expertise, fully applies in the realm of electronic communications, including social media.

7. FOIA and Electronic Communications

In several recent instances, outside groups or governmental agencies have sought to obtain records of faculty members' electronic communications. In 2011, Virginia's attorney general Ken Cuccinelli demanded that the University of Virginia turn over all e-mail messages and other communications related to and produced by former professor Michael Mann, a prominent scientist of climate change, on the grounds that these were public records. The university successfully resisted the request, characterizing the investigation as "an unprecedented and improper governmental intrusion into ongoing scientific research," and charged Cuccinelli with targeting Mann because the attorney general "disagrees with his academic research regarding climate change."[32] But no sooner had this effort been thwarted than a private group, the American Tradition Institute (ATI), filed a FOIA request that mirrored the attorney general's subpoena.

The AAUP and the Union of Concerned Scientists (UCS) filed a joint *amicus* brief in support of UVA and Professor Mann, urging that "in evaluating disclosure under FOIA, the public's right to know must be balanced against the significant risk of chilling academic freedom that FOIA requests may pose." The ATI's request, the brief stated, "strikes at the heart of academic freedom and debate." The organization justified its intervention by claiming that its purpose in seeking the records was to "open to public inspection the workings of a government employee, including the methods and means used to prepare scientific papers and reports that have been strongly criticized for technical errors." The AAUP-UCS brief argued, however, that "in the FOIA context, the public's right to information is not absolute and courts can and do employ a balancing test to weigh the interest of the public's right to know against the equally important interests of academic freedom."[33]

Freedom-of-information laws are generally beneficial: they enhance public knowledge and debate on the workings of government agencies, including public universities. But as the AAUP-UCS *amicus* brief pointed out, in some situations a balance must be struck between competing interests. Likewise, the Supreme Court recognized as long ago as 1957 that politically motivated investigations

---

[31] AAUP, Protecting an Independent Faculty Voice: Academic Freedom after *Garcetti v. Ceballos*, http://www.aaup.org/report/protecting-independent-faculty-voice-academic-freedom-after-garcetti-v-ceballos.

[32] For a summary of events in the Mann case see http://www.aaup.org/our-programs/legal-program/legal-roundup-2012#iii.

[33] Ibid.

of universities and scholars can have a chilling effect on academic freedom.[34] Allowing fleeting, often casual e-mail exchanges among scholars to be subject to inspection by groups bent on political attack raises both privacy and academic freedom concerns. As Committee A previously noted, "The presumption of confidentiality is strongest with respect to individual privacy rights; the personal notes and files of teachers and scholars; and proposed and ongoing research, where the dangers of external pressures and publicity can be fatal to the necessary climate of academic freedom."[35]

For example, in 2011, the Republican Party of Wisconsin filed a FOIA request with the University of Wisconsin, demanding that the university release e-mails from Professor William Cronon, then-president of the American Historical Association, who had criticized the Republican governor's "assault on collective bargaining rights." The administration agreed to release some of Professor Cronon's e-mail messages, excluding "private e-mail exchanges among scholars that fall within the orbit of academic freedom and all that is entailed by it." It also excluded messages that contained student information, and those "that could be considered personal pursuant to Wisconsin Supreme Court case law."

Wisconsin's then-chancellor Carolyn Martin wrote:

> When faculty members use e-mail or any other medium to develop and share their thoughts with one another, they must be able to assume a right to the privacy of those exchanges, barring violations of state law or university policy. Having every exchange of ideas subject to public exposure puts academic freedom in peril and threatens the processes by which knowledge is created. The consequence for our state will be the loss of the most talented and creative faculty who will choose to leave for universities where collegial exchange and the development of ideas can be undertaken without fear of premature exposure or reprisal for unpopular positions.

When such requests are made, faculty members should seek the advice of legal counsel or of the AAUP or ACLU.

8. Defamation

Faculty blog posts, although public and therefore open to all, may be targets of libel actions. In 2013, in separate incidents, the Edwin Mellen Press and its founder sued two university librarians, claiming that negative comments about the press posted by the librarians on the Internet constituted libel. In the first case, Mellen sued an associate librarian at McMaster University in Ontario over a post he had written in 2010, when he had been a member of the library faculty at Kansas State University, that referred to Mellen as a "vanity press" with "few, if any, noted scholars serving as series editors," benefiting largely from the failure of librarians to return books sent for approval at "egregiously high prices." According to the librarian, "As a qualified and experienced librarian, I was sharing a professional opinion for consumption by peers."[36] Although Mellen dropped that suit,

---

[34] *Sweezy v. New Hampshire,* 354 U.S. 234, 250 (1957) ("The essentiality of freedom in the community of American universities is almost self-evident. . . . Scholarship cannot flourish in an atmosphere of suspicion and distrust.")
[35] "Access to University Records," *Academe*, 83, No. 1 (Jan.-Feb., 1997): 47.

[36] "Price of a Bad Review," insidehighered.com, February 8, 2013.

another suit by its founder continued. Mellen threatened legal action against the interim library dean at the University of Utah, after he criticized Mellen, in part for its action against the McMaster librarian. Mellen's threats prompted the Society for Scholarly Publishing to remove the Utah dean's posts from its blog, The Scholarly Kitchen. Such actions constitute clear violations of academic freedom.[37]

Because electronic communications are accessible almost instantaneously around the globe scholars need to be aware that statements they post on blogs or websites or communicate by other electronic means may be subject to the laws of other countries. This fact was highlighted in 2013, when a publisher in India announced its intent to sue for libel a librarian at the University of Colorado at Denver whose popular blog contains a running list of open-access journals and publishers he deems questionable or predatory. On the blog, the librarian accused the Indian publisher of spamming scholars with invitations to publish, quickly accepting their papers, then charging them a hefty publishing fee of nearly $3,000 after a paper was accepted. A letter from the publisher's attorney sought one billion dollars in damages and warned that the librarian could be imprisoned for up to three years under India's Information Technology Act.[38]

Such a suit would likely have little chance of success in U.S. courts, but some other countries' legal definitions of libel are less stringent. (In India allegations of misuse of the Information Technology Act have led the Indian government to modify its rules to make them stricter.) The all-too-common practice of pursuing libel judgments in countries, such as England or Wales, where there is a presumption that derogatory statements are false, has been dubbed "libel tourism." In response, the U.S. Congress in 2010 unanimously passed the SPEECH Act[39], which made foreign libel judgments unenforceable in U.S. courts, unless those judgments are consistent with the First Amendment.[40] However, a judgment unenforceable in the U.S. might still be enforceable in the country where the complaint was filed and which a scholar may need to visit. Those who not only communicate and publish in other countries but whose research or teaching may take them there should be aware of the legal environment governing their expression in those countries.

9. Privacy of Electronic Communications

Electronic communications have greatly enhanced the ability to teach, to learn, and to inquire. Such technologies have made collaboration over great distances much more efficient and enabled people to work more effectively at any hour and almost anywhere. At the same time, the structure of electronic communications technologies can constrain inquiry. Such technologies are designed to document communications and thus amass records of intellectual activities. These records can distort interactions because electronic communications often lack the subtlety of in-person exchanges. They can also be used to investigate individuals in ways that were impossible just a

---

[37] Ry Rivard, "Mellen Press continues its legal maneuvers against critics," *Inside Higher Ed*, April 1, 2013, http://www.insidehighered.com/news/2013/04/01/mellen-press-continues-its-legal-maneuvers-against-critics.
[38] Jake New, "Publisher Threatens to Sue Blogger for $1-Billion," *Chronicle of Higher Education*, May 15, 2013, http://chronicle.com/article/Publisher-Threatens-to-Sue/139243/.
[39] SPEECH is the acronym for the "Securing the Protection of our Enduring and Established Constitutional Heritage" Act.
[40] 124 Stat. 2480–2484.

decade ago. **Privacy in electronic communications is an important means of ensuring professional autonomy and breathing space for freedom in the classroom and for freedom of inquiry. Although privacy is usually framed as an individual right, group or associational privacy is important to academic freedom as well, and to ensuring a culture of trust at an institution.**

When Congress passed legislation to govern the privacy of e-mail and other electronic communications technologies, those technologies were used primarily by businesses. As such, some drew the conclusion that the degree of privacy appropriate to digital communications is substantially lower than that of traditional media. In the intervening years, however, the use of these technologies has blossomed among businesses and individuals alike.

The nature of a communications medium may take some toll on privacy. An institutional computing network legitimately "backs up" some portion of each day's e-mail traffic. In the normal course of events, IT staff members have a degree of access to electronic messages that would be unthinkable for personnel in the university mailroom or on the campus telephone network. By its very nature, electronic communication incurs certain risks that have no print counterpart—for example, the potential invasion of the system by hackers, despite the institution's best efforts to prevent such intrusions. Some of these risks are simply part of the reality of the digital age and of our extensive reliance upon computer networks for the conduct of academic discourse. At the same time, some privacy risks are the product of business imperatives rather than technical necessities.

Privacy risks are likely to increase as institutions are called upon to address more aggressively the security of college and university networks, as researchers increasingly use digital instead of printed resources, and as distance education and electronic communications technologies are more generally relied upon to execute institutional missions.

Faculty members also bear some responsibility for protecting privacy in electronic communications. With the proliferation of BYOD policies, sensitive institutional data are sometimes stored on personal user devices. Thought must be given to how personal and portable devices will be used to access or work with student and research data, in case these devices are compromised, lost, or stolen.

The sensitivity of academic communications and the wide range of scholarly purposes for which digital channels are used warrant a markedly higher level of protection. A fully responsive policy would reflect at least these criteria:

1. The policy should recognize the value of privacy as a condition for academic freedom, and recognize the benefits that privacy and autonomy bring to the individual, to groups, and to the culture of an institution. The institution should recognize that faculty members have a reasonable expectation of privacy in their electronic communications and traffic data.

2. The policy should clearly state that the university does not examine or disclose the contents of electronic communications and traffic data without the consent of the individual participating in the communication except in rare and clearly defined cases. Calls to examine electronic communications or transactional information should consider the special nature of the academy, weigh whether the examination would have disproportionately chilling

effects on other individuals or the institution generally, and contemplate alternative or less invasive approaches to preserve privacy in communications.

3. Employees who operate and support electronic communications resources regularly monitor transmissions for the purpose of ensuring reliability and security of electronic communications resources and services and, in that process, may observe certain transactional information or the contents of electronic communications. Except in specifically defined instances or where required by law, they should not be permitted either to seek out transactional information or contents when those are not germane to system operations and support, or to disclose or otherwise use what they have observed.

4. Faculty should be involved in the setting of institutional policies surrounding the monitoring of and access to content and traffic data in electronic communications. Policies concerning electronic communications should enumerate narrow circumstances where institutions can access traffic logs and content unrelated to the technical operation of these services. If a need arises to access electronic communications data, a designated university official should document and handle the request, and all parties to the communication should be notified in ample time for them to undertake protective measures—save in the rare case where any such delay would create imminent risk to human safety or university property. Accessed data may not be used or disseminated more widely than the basis for such exceptional action may warrant.

5. As reliance on electronic communications technologies grows, more faculty online activities will be subject to being logged or recorded. Institutions are encouraged to use several strategies encapsulated by the idea of "privacy by design" (in which systems and processes are built with the intention of protecting users' privacy) to reduce the risk to free inquiry and association from this logging. These strategies include creating logs at the aggregate (non-personally identifiable) level where possible, carefully controlling access to these logs, removing identifying information from them, and deleting them according to some reasonable retention policy. These strategies must be balanced, of course, to accommodate legitimate security obligations.

Such principles as these, designed as they are to ensure the privacy of electronic communications, will require careful and extensive study by each institution, and the tailoring of specific responses consistent not only with institutional needs and values, but also with state and local law.

10. The Role of Faculty and Shared Governance

Some faculty members mistakenly believe that institutional IT policies are strictly under the purview of the personnel in technology offices, who are thought to possess the requisite expertise to address complex issues relating to network security, provision of bandwidth, outsourcing, and similar matters. But the interests of the faculty are not always consonant with those of IT offices. The latter may be charged, for example, with conserving resources, while faculty members need broad access to information and ideas.

Some technology officers may be tempted to employ software features "just because they can," without full consideration of their implications for academic freedom and learning. For example,

recently developed learning management software allows an institution to disable features that invade privacy. But some technology offices may have a cavalier attitude toward privacy or simply desire to offer all the technological "bells and whistles" available. Hence, electronic communications are too important for the maintenance and protection of academic freedom to be left entirely to such officers. Faculty must participate, preferably through representative institutions of shared governance, in the formulation and implementation of policies governing electronic communications technologies.

However, in order for faculty to play an active and constructive role in the development and execution of such policies, those faculty members who participate in such work need to become more informed about both the technical issues involved and the broader academic freedom implications of their decisions. This report is designed to facilitate that process.

Specifically, we recommend that:

1. Information technology policies and practices should be within the purview of a representative faculty committee. Any new policy or major revision of an existing policy should be subject to approval by a broader faculty body such as a faculty senate.

2. The faculty committee may be drawn from the faculty senate or elected as an ad hoc body by the faculty; its members should not be appointed by the administration.

3. Faculty members who participate in the committee should be familiar with and informed about relevant developments in communications technology so that they are able to recognize potential conflicts with academic freedom principles.

4. The members of the faculty committee should be provided with all relevant contracts and technical materials necessary to make informed decisions about policies governing electronic communications.

5. Faculty must be consulted even when policies are proposed and before administrative actions are taken with respect to information technology that might directly or indirectly implicate academic freedom.

6. In those institutions with collective bargaining, faculty unions should seek to include in their collective bargaining agreements protections for academic freedom in electronic communications as described in this report.

Henry Reichman (History)

California State University, East Bay, *chair*

Ashley Dawson (English)

City University of New York

Martin Garnar (Library)

Regis University

Chris Hoofnagle (Law)

University of California, Berkeley

Rana Jaleel (American Studies)
New York University
Anne Klinefelter (Law and Library)
University of North Carolina
Robert M. O'Neil (Law)
University of Virginia
Jennifer Nichols, *staff*

The Subcommittee