By Virginia Rezmierski and Aline Soules

# Security Anonymity

## The Debate over User Authentication and Information Access

**ANONYMITY: WE WANT IT AND WE DON'T.** We need and want to share our stories, but we also want the details of our lives to remain in our personal control—to release them if and when we decide the time is right, for reasons we determine are worth the loss of a degree of privacy.

As technology expands the way we operate in the electronic environments of colleges and universities—and provides us with new tools for teaching, learning, and research—important ethical issues concerning privacy arise. In this rapidly changing environment, we rarely have the opportunity for in-depth discussion of the different viewpoints on such issues. The push to efficiency, to rapid change, and to application of new technologies often causes key and extremely important issues to be glossed over.

One such issue is whether to require authentication for a user to access electronic resources within a campus environment. Somewhere along the continuum from total security to open access lies a viable path, but getting to that path is not easy. The issue calls for extensive debate, since the questions surrounding resource access in libraries are many and complex. Are incidents of abuse currently happening through or on library networks? What responsibilities and obligations do library professionals have to their users? What responsibilities and obligations do security professionals have to their users? (Sometimes these two groups of users overlap.) What resources in the library are on the networks? How does access to library resources differ from access to other resources on-site

Virginia Rezmierski, Ph.D., is Director, Office of Policy Development & Education, and Adjunct Associate Professor, School of Public Policy, University of Michigan. Aline Soules, M.A., M.S.L.S., is Director, Kresge Business Administration Library, University of Michigan Business School.

Illustration by Scott Roberts

or elsewhere on campus? What are the risks if authenticated access is required? What are the risks if unauthenticated access is allowed?

These questions offer potential for conflict at multiple levels in this debate. At the most basic level are *different responsibilities, different values, and distrust.* As we move on to process, *different experiences and different language* come into play. Once we reach action steps, *logistics and the unknowns of technology* add to the tension. Different opinions about alternatives bring the conflict to the table. The worst scenario is a rush to resolution, causing the trampling of the values and standards of one group for the sake of closure and expedience. This can leave a campus without coherence and the required cooperation.

## Different Responsibilities, Different Values, and Distrust

*Librarians' Responsibilities*
Librarians have long been among the staunchest defenders of First Amendment rights. They care deeply about, and feel responsible for, protecting user privacy and providing access to uncensored information in a manner that is as barrier-free as possible. William Oldfield, in his article "Secure Public Internet Access," states:

> *Free, open, and equitable access to information has always been a primary tenet of library service. An informed citizenry is a cornerstone of our democracy. In a time when "learning a living" has become a fact of the workplace, access to information is essential for ensuring equal opportunity for citizens. Students without access to the new electronic information resources on the Internet, for example, are disadvantaged. Providing barrier-free, public access to the information resources on the Internet should be a top priority for every library.*[1]

Note, particularly, the words "free," "open," "equitable," and "barrier-free." Librarians are further supported in this set of obligations by the "Code of Ethics" of the American Library Association (ALA), which includes the following among its statements:

- We provide the highest level of service to all library users through appropriate and usefully organized resources; equitable service policies; equitable access; and accurate, unbiased, and courteous responses to all requests.
- We uphold the principles of intellectual freedom and resist all efforts to censor library resources.
- We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired, or transmitted.
- We recognize and respect intellectual property rights.

The question within networked environments is how to meet these obligations.

*Security Professionals' Responsibilities*
Security professionals also carry obligations and responsibilities. They are charted with protecting the electronic systems and networks from unauthorized access, abuse, disruption, tampering, and failure. They are responsible for ensuring that the intellectual property of faculty and students in their communities is protected against unauthorized access or modification. They are accountable for protecting systems against overload and misuse. They monitor loads and use statistics and provide backups and disaster recovery plans. They must cope with, and protect against, the increasingly sophisticated denial-of-service attacks. Such attacks are growing because of their potential, within networked environments, to shut down entire systems and even organizations through commands delivered from remote locations.

Although a more loosely formed professional group, security professionals are also supported by professional codes of ethics. The "Code of Ethics" of the Association for Computing Machinery (ACM), for example, includes the following statements:

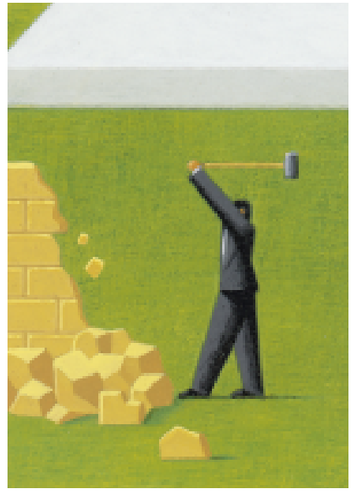
- An ACM member should consider the health, privacy, and general welfare of the public in the performance of his work.
- An ACM member, whenever dealing with data concerning individuals, shall always consider the principle of the individual's privacy and seek the following:
  - To minimize the data collected
  - To limit authorized access to the data
  - To provide proper security for the data
  - To determine the required retention period of the data
  - To ensure proper disposal of the data

In concert with their recognized responsibilities, the two groups hold different views on the fundamental values of privacy, access without charge, and equity of access.

*Privacy*
In most states, state laws protect the privacy of users by prohibiting the release of library lending information to third parties. In Michigan, there is further protection of this information, even from disclosure under the Freedom of Information Act (FOIA).

Security professionals also support privacy of lending records but argue for user authentication when accessing a network. Authentication provides assurance that the individual is authorized to use the university's resources and that it is possible to identify individuals accused of system abuse or illegal activity. Generally, security professionals need to look only at basic machine-identification information and network time-stamps to discern the source of an abuse and who was using the source machine at the time. They are not interested in what a particular individual was accessing or reading when an abuse was committed.

Once authentication logs are maintained, however, both groups agree that the ability to draw conclusions about the services used by an individual may incriminate or otherwise be used against him or her, thus reducing the degree of freedom. Some library services are already tied to authentication, for example, an electronic resource bound by contractual agreement or a physical resource checked out for use. Librarians resist implementing such requirements, however, and object to wide-scale application of authentication because it is the "slippery slope" that leads to the loss of an essential freedom. Security professionals believe that this is a small price to pay in a networked environment, where one person's abuse can affect or deny others' access to resources.



*Access without Charge*
For many librarians, access without charge means people will not pay to access resources of public or publicly funded libraries. Users should be able to read any materials without fees. This emphasis on free access is further extended for libraries designated as Federal Depository Libraries, which are obligated to provide government information at no cost to the general public. The right to information is an essential part of a free society.

Most security professionals support the concept of free access and recognize the importance that information access holds for a free society. However, as part of a workforce that sees more than 10 percent of overall organizational budgets being committed to the introduction and support of technology, they note that no resource can be truly "free." The university must pay to provide the networks, hardware, and software on which resources reside. Security professionals, therefore, are obligated to protect resources against tampering, to ensure that networks are operating, and to maintain and protect systems. In that way, resource use can be implemented free of additional charge and made available to all.

*Equity of Access*
For librarians, "equity of access" means that there should be no restriction on who can access resources and that no one person, by virtue of privilege or experience, should have more access to public information than another person. The information technology environment has increased librarians' concerns about equity of access as the gap between "haves" and "have-nots" has increased. Public colleges and universities, especially those designated as Federal Depository Libraries, include in their definition of *user* any walk-in citizen, regardless of his or her affiliation with the institution. Since the resources of the library now extend well beyond print materials on physical shelves to resources in many electronic forms, this definition of *user* is a significant source of conflict between librarians and security professionals.

Security professionals agree that equity of access is important—but only for certain resources on campus. In their view, the population to be protected is the specific community identified through enrollment, employment, or designated membership. Denial of service can result from service attacks and misuses or abuses of the networks; therefore, fair and equitable access to resources starts with adequate protection of systems. Security professionals also think that not all resources on campus should be equal in terms of access. Although laboratories and classrooms, for example, are also provided through public funds within public institutions, they are established for specific purposes and missions; therefore, unauthorized individuals are denied access.

**For librarians, "equity of access" means that there should be no restriction on who can access resources and that no one person, by virtue of privilege or experience, should have more access to public information than another person.**

*Distrust*
These differing values and responsibilities of librarians and security professionals can lead to distrust between the two groups. When librarians hear security professionals explain how a hacker can be traced through the networks, they fear for their users and the privacy that they value so highly. When security professionals hear librarians talk about

the low rate of abuses in the library, they conclude that librarians are unaware of the severity of the problem and fear for the security that they value so highly.

In addition, the different work environments of the two groups may add to this distrust. Psychologists such as Erik Erickson,[2] Abraham Maslow,[3] and many others have described the importance of consistency and predictability in life and how those factors lead to the development of trust. In our current information technology environments, consistency and predictability are hardly applicable words. For librarians, years of experience with the organization and management of resources have led to well-established policies and procedures and a generally accepted and consistent set of articulated values. These continue to provide a foundation even as librarians function in a more rapidly changing environment. Security professionals, however, have no such consistencies. Their newer, less established environment is even more unstable and subject to change than the library environment, and they are expected to manage diverse and often incompatible systems. The rate of growth and the direction of new innovations are unpredictable and chaotic. There is a considerable difference between the measured, methodical approach of libraries and the experimental, risk-management approach of systems.

### Different Experiences and Different Language

The different experiences and the resulting different language of these two groups can lead to major miscommunication. One area of divergence involves the perception of resource abuse on campus. Librarians perceive the percentage of abuse relative to the whole population to be low. They think that the community should not be given restrictions or new barriers because of the unacceptable behavior of one or two individuals. Security professionals, on the other hand, know that it takes only one incident to create a significant, even threatening situation. This is perhaps the driving force leading security professionals to seek authenticated access to electronic resources. Do incidents happen from unauthenticated library machines networked to the campus and the World Wide Web? A small sample from our campus incident logs may help answer this question:

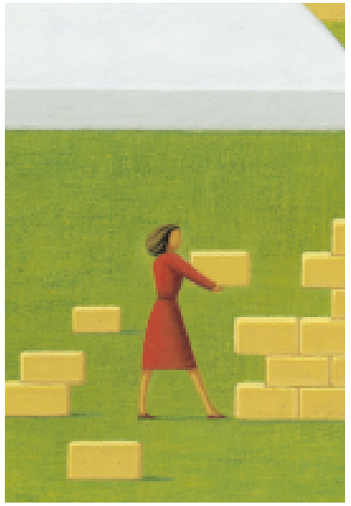
- A student used a Telnet session and a library computer to crack into another university's network. On the second occasion, a system administrator identified the linkage as the same and located its source.
- From an unauthenticated library machine, a student posted, to various news groups, several e-mail messages encouraging readers to call a specific individual at another university, an individual with whom he had a conflict. The student gave readers the name and work telephone number and urged them to call and harass the individual.
- A student complained to the university that her account had been compromised. She had received from a stranger the answer to a question she had posed to another person. The student had sent e-mail from a library machine and had not signed off completely.
- A graduate student received a highly offensive, racially targeted e-mail from a library machine. Without authentication, the sender could not be identified.
- A famous hotel resort received a bomb threat from one of the university library's public-access machines. The police asked the university to determine who had been using the machine at the time the bomb threat was posted, but since the machine did not require authentication and was open to the public, this could not be done.

Incidents of inappropriate and abusive use—through Telnet, gateways, and e-mail—and threats to individuals and institutions happen from unauthenticated library machines. In a recent meeting of state universities and law enforcement personnel, representatives were asked for examples of electronic threats occurring on their campuses. All campus representatives noted that they had seen an increase in such activity, in the form of direct threats to individuals, bomb threats, and other threats to institutional facilities. All representatives indicated that such activity most often occurred from unauthenticated machines in campus libraries.

Security professionals know about and have experience with such activity. Librarians, on the other hand, do not generally hear about these incidents within electronic environments. They do have experience with such incidents in the print world, however. In that environment, detection gates and security strips are used, and some libraries have chosen to mount mirrors or video cameras, depending on the outcome of their in-house debate on values. The print world, however, still does not permit as systematic and comprehensive a check as is possible in the electronic world. Libraries feel comfortable with, or have adjusted to the idea of, these physical security devices and still believe that they isolate the offender rather than creating barriers to, or invading the privacy of, all users.

There is also an important difference in language here. For security professionals, the term *security* has several understood components, known by the acronym IAA—identification, authentication, authorization. For them, *security* means that you can identify a person (identification), confirm that the person is who he or she says (authentication), and confirm that if the person can access resources, he or she has a legitimate right to do so (authorization). For security professionals, IAA is critical to ensuring the reliability and availability of services. Librarians are also concerned about the availability and preservation of resources, but they do not tie their ideas of security (protection against theft and destruction) to IAA processes. The concept of IAA, as defined by security professionals, runs contrary to library values. In addition, such security parameters were not considered in that way for traditional library resources. If IAA concepts were applied to such resources, high-level security would be considered valid only for the protection of some rare or irreplaceable physical resources.

Another language difference arises with the term *barrier.* For many librarians, a barrier is anything that keeps people—physically or psychologically—from open access to library resources. For example, a log-in/password process for guests is a form of barrier and is, therefore, to be avoided. One of librarians' complaints is that within the electronic environment, more barriers have been forced on their users. These include barriers that are introduced in negotiated contracts with publishers and aggregators, barriers that occur when users must negotiate across incompatible computer systems to get available resources, and barriers that arise if fees are collected for printing from electronic resources. Although some librarians do not recognize the ways in which they have already implemented some form of IAA into their services, many see the values of privacy and barrier-free access being chiseled away. When security professionals talk of yet more barriers that are needed to implement IAA mechanisms systemically and systematically, librarians want to take a stand against further intrusion.



**Once a user gains access through an unauthenticated library machine, the user may be able to access any number of resources on the campus, resources that are underprotected and that are unassociated with library holdings.**

Security professionals, however, argue that by placing resources on networks, librarians have already increased barriers. Individuals must learn how to use computers, how to access information remotely, how to type, and how to print. Although librarians recognize this, they argue that this is all the more reason not to introduce additional barriers. But for security professionals, barriers are more akin to fire walls—true attempts to keep people out rather than devices to slow or alter the direct line of access to a resource. A log-in/password process simply facilitates open access by ensuring that the resource is protected, reliable, not subject to abuse, and, therefore, available when needed.

### Logistics and the Unknowns of Technology

The crux of the conflict between librarians and security professionals arises most clearly when library collections and other resources are placed on networks. For librarians, networked resources are part of basic library holdings. Only the format has changed. The holdings have expanded and are now located in different places. Access should have no more barriers than are required for any other type of information. Security professionals, however, point out that these are not the only information collections or services available through the network. Once a user gains access through an unauthenticated library machine, the user may be able to access any number of resources on the campus, resources that are underprotected and that are unassociated with library holdings. The idea that users could access certain protected collections of information without authorization causes concern. Librarians respond by suggesting that nonlibrary resources should be protected separately from library resources and that a technical solution should be found to do this.

It is possible to protect resources by requiring authentication at the resource itself. Library users would be able to get on the network at any one of several points without identifying themselves and could gain access to many freely available resources; but when they want to enter a contractually protected library resource, an authentication mechanism would ensure that only those who meet the contractual requirements would be allowed to enter. The difficulty with this system is that users complain when they face constant and repetitive authentication processes as they move back and forth among multiple resources. The possibility of a single search protocol across multiple library databases also renders this option less viable.

In complex environments, where many resources are adequately protected and others are not (e.g., profes-

sors' or students' collections of writings, college or university services, departmental administrative data, individual information), another way of protecting resources is to require authentication at the network level, that is, at the point of entry or log-in. Even with this method, the complexity of networks and the number of diverse devices being added to them may make it impossible to protect many resources at the present time. Security professionals believe that authentication at the point of network access is necessary and that for highly protected resources, re-authentication or confirmation of previous authentication at the resource level is also required to ensure the desired level of availability for that resource.

### Policy-Making and Implementation

Both librarians and security professionals are concerned, in very different ways, about privacy and the protection of the individual. Both groups are sincerely trying to fulfill their responsibilities to the community they serve. For a policy to be effective in guiding community behaviors, it must reflect the full range of the community's values, must be understood and embraced by community members, and must reinforce the most important values and the mission of the institution as a whole. An effective policy requires campus-wide discussion and the involvement of each of the major constituencies of the community. Extremism and entrenchment must be avoided.

On the continuum from total security to open access, polar positions inhibit functioning. Total security makes systems unusable. Completely open access provides no security. Where is the right balance point for the community? To answer this question, we must consider other questions:

- To whom do we wish to give access and why?
- How can we provide that access technically?
- How can we provide that access contractually, for example, to third-party, for-fee information resources?
- How can we provide that access legally?
- How can we ensure data integrity where required?
- What information should be preserved for the future, and how can we achieve preservation?
- How do we protect individual privacy?
- How do we protect individuals from unwanted or unwarranted intrusion into personal information?
- How do we balance the needs for access to information (users), protection of information (creators), and cost recovery for providing information (publishers)?
- How do we articulate a comprehensible and comprehensive policy that will enable us all to work?
- How do we ensure good communication, the development of a common language, ongoing discussion that does not falter in moments of crisis, and a balanced policy that meets many diverse needs and values?
- How do we deal with the authentication issue
  (1) at the network level and at the resource level, using log-in/password and guest passwords for noncommunity members (high barrier),
  (2) at the network level only (medium barrier),
  (3) at the resource level only (medium barrier), or
  (4) at no level, that is, no authentication (low barrier)?

To begin to decide what solutions would best balance the values and needs of these two groups of professionals, we should first sample incidents that occur from unauthenticated library computers. The next step is to gather statistics that show the volume of use of various services such as HTTP, STMP, POP3, Telnet, and ftp. These data can help to identify services that could be removed from unauthenticated-access machines to reduce vulnerability. The final step is to examine the types of services offered in the traditional library environment and those offered in the electronic environment with a view to comparing the driving forces that lead to some form of protection for those resources and the nature of the protection that is currently being implemented. It is helpful to identify these protections in terms of the IAA components described earlier. These sources of information will help maintain a focus for critical discussions and policy development.

Regardless of the results of data analysis or debate, we all must understand the process and the issues. For any process to be successful, communication must be open and continuous. The parties involved must keep talking, keep listening, and keep questioning. This is particularly true when there are different responsibilities and values, distrust, different experiences and language, different logistics, and incomplete knowledge about technology.

Critical questions are yet to be answered. How do we reconcile the belief in freedom of information, freedom of access, freedom from monitoring and censorship, and protection of privacy with the need to maintain integrity of resources, protect individuals from unwanted and unwarranted intrusion, assure creators of information that their data will not be compromised, and ensure that the copyright belonging to creators and publishers of information will be protected? Legally, how do we reconcile the varying requirements of FERPA (Family Educational Rights and Privacy Act), FOIA, Lending Records laws, Federal Depository obligations, copyright law, and the myriad laws that are now being created around the communications and computer industries? This, of course, presumes that we all agree about how those laws are interpreted, which is clearly not the case.

How do we create a policy in light of changing technology? What are the technical options, who understands them fully, what will come tomorrow, and how will we create any kind of strategy, direction, or lasting policy amid such change? How should we establish responsibility for content validity and reliability? What belongs to the institu-

**How do we reconcile the belief in freedom of information, freedom of access, freedom from monitoring and censorship, and protection of privacy with the need to maintain integrity of resources, protect individuals from unwanted and unwarranted intrusion, assure creators of information that their data will not be compromised, and ensure that the copyright belonging to creators and publishers of information will be protected?**

tion and what to the information provider? At the moment, the concept is that responsibility for content validity and information preservation should be at the local level. But do all creators of information have the technology and financial resources to accept this responsibility? If not, does the information remain vulnerable, or does someone else take over that responsibility?

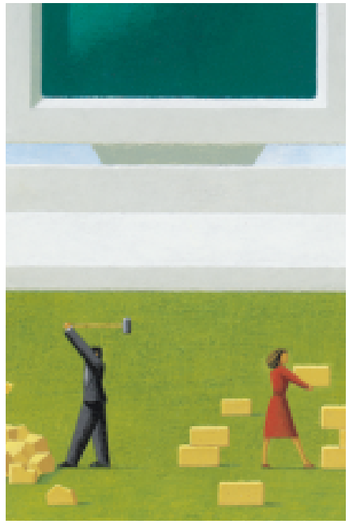
Some options exist. Though not all are compatible with the others, and they fall at various points on the continuum between full security and open access, the following suggestions offer guidelines:

- In library settings, provide machines that require authentication either by community individuals or through guest log-in/password processes with built-in expiration dates/times.

- Place guest or unauthenticated library machines in one or two sites that will facilitate the logistics of managing guest log-in/passwords or will at least permit easier physical observation.

- Provide an aggressive educational campaign to encourage responsible and legal use of campus information resources.

- Create a campus policy that allows libraries and other campus units with a mission that precludes full authentication to offer unauthenticated access, but require those units to spell out the actions they will take to protect other campus resources from misuse—for example, providing the name of a person to call in case of abuse.



- Provide "authenticated access only" on all library machines, and support that action with stringent policies and procedures for disciplinary actions against anyone who violates user privacy and with policies that direct data-disposal schedules and the conditions under which data could be released to third parties—for example, with court order.

- Provide machine logs for activities on all library machines, but have the logs maintained and retained for a short duration by library rather than system personnel.

- Initiate and lead an effort to have machine logs included under the legal protections afforded to traditional library user data.

- Remove certain functions (e.g., e-mail) from unauthenticated library machines in order to reduce potential network vulnerabilities.

**Conclusions**

We would not have found the time to examine these issues so carefully had we not come to a near impasse in attempting to write policy about authentication for electronic resources on our own campus. In the midst of frustration, a mounting sense of urgency, intensely held but differing values, a sense of responsibility based on different perspectives, a lack of understanding of variant viewpoints, and a lack of knowledge about technical possibilities, we experienced a breakdown in communication, followed by an entrenchment in viewpoints. A full solution has not yet been found; however, the issues that emerged have expanded our understanding of underlying values and have broadened our appreciation for the professionalism and objectives of both librarians and security professionals.

There are clearly many questions and no easy answers. The opportunity for debate on this important ethical issue lies before us. The keys to success lie in maintaining balance and continuing discussions. Whatever happens, keep talking!

**Notes**

1. William Oldfield, "Secure Public Internet Access," *ACCESS* 3, no. 2 (winter 1997).
2. E. Erickson, *Childhood and Society*, 2d ed. (New York: Norton, 1963).
3. A. H. Maslow, *Motivation and Personality* (New York: Harper and Row, 1954).