Enabling Access in Digital Libraries
A Report on a Workshop on Access Management

Executive Summary

The increasing amount of digital information now readily generated and easily available presents the information management community with a wide-reaching and complex set of challenges. This report presents the discussions and outcomes of a workshop on a subset of the challenges affecting many members of that community: policy makers involved in making decisions on managing digital data in relation to questions of privacy; legal experts who draft contracts and licenses which must be implemented through technical mechanisms for authentication and authorization; technologists designing new software for controlling electronic use and mis-use; and publishers and librarians who, as major providers of information, play a central role in striking a balance between protecting copyright and providing access to the cultural record of knowledge. Indeed, the principal focus of this particular workshop was on the means of managing access to published knowledge in digital form within the context of the research library. However, the specific focus taken here merely emphasizes the much larger dimensions of access management issues. In the bigger picture, as the digital age continues to advance rapidly, all citizens must be concerned with issues of privacy, protection, authorization, and authentication.

Consider the following questions:

How can someone who claims to be a member of a company or university that has licensed an electronic journal or other digital forms of knowledge be verified in order to get access to the contents? How is a system to know that the staff member, professor, or student is not someone else? Will systems be capable of screening out imposters?

How finely can information providers discriminate among potential users when making their materials available? What principles should guide organizations, such as universities and public libraries, in deciding who should be authorized to have access to a database of published information, such as the on-line version of the New York Times? What options do public libraries have to be able to authorize use of licensed materials to the general citizenry that they serve?

How will authors and creators of the cultural record themselves be protected from digital thievery? Will Garrison Keillor be correct in warning that authors on the information superhighway will become "the deer in the headlights" of a vast traffic they cannot control? [1] What means do custodians have available to them to ensure the accessibility of the cultural record while protecting the property interests of the authors and creators against users copying the information to disk and redistributing it or making hundreds of printed copies?

Should digital data itself be specially marked with a digital lock so that only users who have matching keys can gain access? How does such a mechanism accord with constitutional and legislative mandates to balance the need to protect the rights of authors and creators against the need to make the cultural record of knowledge readily available?

These pressing questions were among the issues addressed by a selected group of expert practitioners and researchers from several disciplines at a one day meeting held on April 6, 1998 at the Brookings Institute in Washington, D. C. The meeting was jointly sponsored by two groups who are actively involved in seeking solutions: the Digital Library Federation (DLF), which consists of major research libraries and archives in the U.S., and the Information and Intelligent Systems Division of the Computers, Information Sciences and Engineering Directorate of the National Science Foundation (NSF).

This report presents the discussions of the workshop and summarizes the conclusions reached. Among its conclusions, the workshop yielded several results. It identified a need for focus in research and project evaluation in two key areas:

System usability: significant attention must be given to understanding the ways that users interact with systems and what their needs are given new information types and the functionality of these types in the emerging digital environment;

Economic models: innovation is needed in the metrics used to measure usage of digital resources and in the development of pricing schemes and payment mechanisms based on such metrics;

The workshop also resulted in specification of five key properties for the design and adoption of systems that enable access for users while respecting the rights and interests of authors and publishers:

Simplicity: the less complex a system of access management is the more readily it can be adopted technologically and organizationally, and the more acceptable it is to all involved in its implementation.

Privacy: systems that manage access to the cultural record of knowledge must preserve the privacy of users against detailed tracking and disclosure of use. Privacy of users is an essential value that cannot be compromised.

Good Faith: access management agreements rely on good faith dealing among the parties, who each would prefer to depend, in the systems that implement these agreements, on reasonable barriers against abuse rather than complex restrictions that inhibit use.

Trusted Intermediaries. Intermediaries play an essential role in providing access to the cultural record as trusted parties by users and providers, and as efficient aggregators of distribution and usage. System design must account for the role of such intermediaries.

Reasonable Terms: access management systems must reasonably distinguish between access and use. Management of access cannot always reliably predict, and may inappropriately constrain uses of information, especially in teaching and research contexts. The most useful access management system will not limit access to known users, but will be reasonably open to the possibility of serving unlikely users.

The outcomes of this workshop relate specifically to the problems of managing access to the cultural record in digital form for research and teaching purposes. Yet the solutions proposed in this workshop for enabling appropriate and continuing access to digital repositories also apply in other realms, including those involving access to much more highly sensitive information in the form of digitally produced and maintained business records, medical records, insurance information, credit card data, and logfiles from web-browsers. And enabling appropriate access to all these various forms of digital information requires the concerted effort and talent of many stakeholders, including information specialists, librarians, publishers, computer scientists, lawyers, scientists, and policymakers, as well as the general citizenry.