

1 State of the Art

Digital preservation consists of the processes aimed at ensuring the continued accessibility of digital materials. ... To achieve this requires digital objects to be understood and managed at four levels: as physical phenomena; as logical encodings; as conceptual objects that have meaning to humans; and as sets of essential elements that must be preserved in order to offer future users the essence of [each] object.

Webb 2003, *Guidelines for the Preservation of Digital Heritage*

Information interchange is a growing activity that is beginning to be accompanied by attention to preserving digital documents for decades or longer—periods that exceed practical technology lifetimes and that are sometimes longer than human lifetimes. In the industrial nations, nearly every business, government, and academic document starts in digital form, even if it is eventually published and preserved on paper. The content represents every branch of knowledge, culture, and business. Much of it is available only in digital form, and some of this cannot be printed without losing information.

Today's information revolution is the most recent episode in a long history of changes in how human knowledge is communicated. Most of these changes have not eliminated communication methods that preceded them, but instead have supplemented them with means more effective for part of what was being conveyed. However, they have stimulated, or at least amplified, social changes to which some people have not adapted readily, and have therefore resisted. A consequence has been that such changes did not become fully effective until these people had been replaced by their progeny. Much of the literature about today's information revolution and its effects on durable records suggests that this pattern is being repeated.

The driving forces of information revolutions have always been the same: more rapid transmission of content, more efficient means for finding what might be of interest, and improved speed and precision of record-keeping. Today's revolution is so rapid that it might startle an observer by its speed. Part of what is communicated is technology for communication. This helps those who want to exploit the new technical opportunities to do so more quickly and with less effort than was needed in previous information revolutions. The phenomenon is familiar to chemists, who call it autocatalytic reaction.

The full infrastructure required to absorb revolutionary changes does not all come into place simultaneously. People's enthusiasm for the most obvious and most readily exploited aspects of new technology—in this case the advantages of digital documents over their paper counterparts—

can cause them to change their habits before essential infrastructure is deployed—in this case services to preserve their digital works for as long as they might want. Perhaps people have not noticed and will not notice that there is no preservation infrastructure until they personally lose digital documents they thought would be accessible into the distant future. Prominent technical and operational issues that people might be assuming have already been adequately taken care of, but which have not, include management of assets called “intellectual property” and management of digital repository infrastructure.

1.1 What is Digital Information Preservation?

Almost all digital preservation work by scholars, librarians, and cultural curators attempts to respond to what is called for in a 1995–1996 Task Force Report:

[T]he Task Force on Archiving of Digital Information focused on materials already in digital form and recognized the need to protect against both media deterioration and technological obsolescence. It started from the premise that migration is a broader and richer concept than “refreshing” for identifying the range of options for digital preservation. Migration is a set of organized tasks designed to achieve the periodic transfer of digital materials from one hardware/software configuration to another, or from one generation of computer technology to a subsequent generation. The purpose of migration is to preserve the integrity of digital objects and to retain the ability for clients to retrieve, display, and otherwise use them in the face of constantly changing technology. The Task Force regards migration as an essential function of digital archives.

The Task Force envisions the development of a national system of digital archives ... Digital archives are distinct from digital libraries in the sense that digital libraries are repositories that collect and provide access to digital information, but may or may not provide for the long-term storage and access of that information. The Task Force has deliberately taken a functional approach [to] ... digital preservation so as to prejudge neither the question of institutional structure nor the specific content that actual digital archives will select to preserve.

The Task Force sees repositories of digital information as held together in a national archival system primarily through the operation of two essential mechanisms. First, repositories claiming to serve an archival function must be able to prove that they are who they say they are by meeting ... criteria of an independently administered program for archival certification. Second, certified digital archives will have available to them a critical fail-safe mechanism. Such a mechanism, supported by organizational will, economic means, and legal right, would enable a certified archival repository to exercise an aggressive rescue function to save culturally significant digital in-

formation. Without the operation of a formal certification program and a fail-safe mechanism, preservation of the nation's cultural heritage in digital form will likely be overly dependent on marketplace forces.

Garrett 1996, *Preserving Digital Information*, Executive Summary

Ten years old, this report still provides excellent guidance. However we have learned to modify two technical aspects of the quoted advice.

First of all, the task force report overlooks that periodic migration of digital records includes two distinct notions. The first, faithful copying of bit-strings from one substratum to a successor substratum, is simple and reliable. In fact, such copying functionality is provided by every practical computer *operating system*. The second, copying with change of format from a potentially obsolete representation to a more modern replacement, is a complex task requiring highly technical expertise. Even then, it is error-prone. Some potential errors are subtle. Preservation with the assistance of programs written in the code of a virtual computer, described in Chapter 12, minimizes such risks.

A second concern is that periodic certification of an institutional repository as satisfying accepted criteria cannot reliably protect its digital holdings against fraudulent or accidental modification that destroy the holdings' authenticity and might harm eventual users. Ten years after the report suggested the pursuit of reliable digital repositories, no widely accepted schedule of criteria has been created. A fresh attempt to do so began in 2005. In contrast, a widely known cryptographic procedure can protect any digital information with evidence with which any user can decide whether the information is reliably authentic (Chapter 11).

What will information originators and users want? Digital preservation can be considered to be a special case of communication—asynchronous communication which the information sent is not delivered immediately, but is instead stored in a repository until somebody requests it. An information consumer will frequently want answers that resolve his uncertainties about the meaning or the history of information he receives. Digital preservation is a case of information storage in which he will not be able to question the information producers whose work he is reading.

Digital preservation system designers need a clear vision of the threats against which they are asked to protect content. Any preservation plan should address the threats suggested in Table 2.¹¹

¹¹ Adapted from Rosenthal 2005. *Requirements for Digital Preservation Systems*.

Table 2: Generic threats to preserved information

Media and Hardware Failures	Failure causes include random bit errors and recording track blemishes, breakdown of embedded electronic components, burnout, and misplaced off-line HDDs, DVDs, and tapes.
Software Failures	All practical software has design and implementation bugs that might distort communicated data.
Communication Channel Errors	Failures include detected errors (IP packet error probability of $\sim 10^{-7}$) and undetected errors (at a bit rate of $\sim 10^{-10}$), and also network deliveries that do not complete within a specified time interval.
Network Service Failures	Accessibility to information might be lost from failures in name resolution, misplaced directories, and administrative lapses.
Component Obsolescence	Before media and hardware components fail they might become incompatible with other system components, possibly within a decade of being introduced. Software might fail because of <i>format obsolescence</i> which prevents information decoding and rendering within a decade.
Operator Errors	Operator actions in handling any system component might introduce irrecoverable errors, particularly at times of stress during execution of system recovery tasks.
Natural Disasters	Floods, fires, and earthquakes.
External Attacks	Deliberate information destruction or corruption by network attacks, terrorism, or war.
Internal Attacks	Misfeasance by employees and other insiders for fraud, revenge, or malicious amusement.
Economic and Organization Failures	A repository institution might become unable to afford the running costs of repositories, or might vanish entirely, perhaps through bankruptcy, or mission change so that preserved information suddenly is of no value to the previous custodian.

These threats are not unique to digital preservation, but the long time horizons for preservation sometimes require us to take a different view of them than we do of other information applications. Threats are likely to be correlated. For instance, operators responding to hardware failure are more likely to make mistakes than when they are not hurried and under pressure. And software failures are likely to be triggered by hardware failures that present the software with conditions its designers failed to anticipate or test.

Preservation should be distinguished from conservation and restoration. *Conservation* is the protection of originals by limiting access to them. For instance, museums sometimes create patently imperfect replicas so that they can limit access to irreplaceable and irreparable originals to small numbers of carefully vetted curators and scholars. *Restoration* is the creation of new versions within which attempts have been made to reduce

damage.¹² Because audiovisual (A/V) media are so easily damaged and because most A/V documents older than about ten years were recorded as analog signals, restoration is used by broadcasting corporations that plan to replay old material.

1.2 What Would a Preservation Solution Provide?

What might someone a century from now want of information stored today? That person might be a critic who wants to interpret our writings, a businessman who needs to guard against contract fraud, an attorney arguing a case based on property deeds, a software engineer wanting to trace a program's history, an airline mechanic maintaining a 40-year-old airframe, a physician consulting your medical charts of 30 years earlier,¹³ or your child constructing a family tree.¹⁴ For some applications, consumers will want, or even demand, evidence that information they depend on is authentic—that it truly is what it purports to be. For every application, they will be disappointed by missing information that they think once existed. They will be frustrated by information that they cannot read or use as they believe was originally intended and possible.

To please such consumers and other clients, we need methods for

- ensuring that a copy of every preserved document survives as long as it might interest potential readers;
- ensuring that authorized consumers can find and use any preserved document as its producers intended, without difficulty from errors introduced by third parties that include archivists, editors, and programmers;
- ensuring that any consumer has accessible evidence to decide whether information received is sufficiently trustworthy for his applications;
- hiding information technology complexity from end users (producers, curators, and consumers);
- minimizing the costs of human labor by automatic procedures whenever doing so is feasible;
- enabling scaling for the information collection sizes and user traffic expected, including empowering editors to package information so as to avoid overloading professional catalogers; and

¹² Hess 2001, *The Jack Mullin/Bill Palmer Tape Restoration Project*, illustrates restoration.

¹³ Pratt 2006, *Personal Health Information Management*.

¹⁴ Hart 2006, *Digitizing hastens at microfilm vault*, describes a family tree of unusual size and importance to the participants—the genealogical files of the Church of Jesus Christ of Latter Day Saints. Digitization is occurring primarily to provide ready access, rather than for preservation. However, some of the images are on acetate film, which is being rewritten to polyester film.

- allowing each institutional and individual participant as much autonomy as possible for handling preserved information, balancing this objective with that of information sharing.

Many institutions already have digital libraries, and will want to extend their services to durable content. They will want to accomplish this without disruption, such as incompatible change from their installed software.

Information producers will want to please consumers, and archive managers will want to please both producers and consumers. Archive managers are likely to have sufficient contact with producers to resolve information format and protocol issues, but will have personal contact with only a small fraction of their consumer clients.

Information consumers will decide whether to trust preserved information usually without conversations with producers or archivists. Each consumer will accept only a few institutions as origins in a trust graph—perhaps fewer than 20 worldwide for scholarly works. He will trust the machinery under his own control more than he trusts other infrastructure. He will see only information delivered to his local machine.

Digital information might travel from its producer to its consumer by any of several paths—not only using different Internet routes, but also involving different repositories. Which path will actually be used often cannot be predicted by any participant. Consumers, and to some extent also producers, will want the content and format of document instances they receive, or publish, to be independent of the route of transmission.

When a repository shares a holding with another repository—whatever the reason for the sharing might be—the recipient will want the delivery to include information closely associated with that holding. It will further want a ready test that everything needed for rendering the holding and for establishing its authenticity is accessible.

1.3 Why Do Digital Data Seem to Present Difficulties?

We can read from paper without machinery, but need and value mechanical assistance for digital content access for at least the following reasons:

- machinery is needed for content that paper cannot handle, such as recordings of live performances;
- much of every kind of information management and communication can be reduced to clerical rules that machines can execute and share much more quickly, cheaply, and accurately than can human beings;
- we are generating far more content than ever before, want to find particular information rapidly, and want to preserve more than ever before; and

- high performance and reliability depend on complex high-density encoding.

Digital information handling that many people older than 40 years find unnatural and difficult is accepted as natural and easy by many in the next generation. Many of us have personal experience with that. An anecdote might provoke a smile as it illustrates the point. A man was puzzled by a photograph showing six toddlers, each in a big flowerpot and wearing a wreath. He was amazed that every child was smiling and looking in the same direction. He mused aloud, “How did the photographer get them all to sit still simultaneously?” His teenage daughter looked over his shoulder. “Simple, Dad. They just clicked them in!”

A factor in comparisons between reading from paper and exploiting its digital counterpart is our education. We each spent much of our first ten years learning to write on and read from paper. Our later schooling taught us how to write well and interpret complex information represented in natural language. However, as adults we tend to be impatient with whatever effort might be needed to master the digital replacements. In contrast, many of our children are growing up comfortable with computing ideas.

In addition, our expectations for the precision and accuracy of modern information tend to be higher than ever before. Our practical expectations (for health care, for business efficiency, for government transparency, for educational opportunities, and so on) depend more on recorded information than ever before. All these factors make it worthwhile to consider structuring explicit digital representations of shared experience, language, world views, and ontologies implicit in our social fabric. The reliability and trustworthiness that can be accomplished with digital links are much better than what is possible in paper-based archives—an example of technology contributing to rising expectations.

Human beings accept a great deal of vagueness in their communication. This is partly because they have the opportunity to inquire whenever ambiguity proves troublesome. Such inquiry for computer programs is not usually possible, a fortiori not possible for preserved digital objects. For such information, if potential sources of confusion are to be avoided, this must be done before most users might want to ask questions. The care needed with digital technology has a reward, frequently bringing to light previously unnoticed ambiguities, omissions, and other problems, and teaching us to improve the precision with which we speak.

1.4 Characteristics of Preservation Solutions

Whatever preservation method is applied, the central goal must be to preserve information integrity; that is, to define and preserve those features of an information object that distinguish it as a whole and singular work.

Garrett 1996, *PDITF* p.12

The *Reference Model for an Open Archival Information System* (OAIS) is a conceptual framework for organizations dedicated to preserving and providing access to digital information over the long term. An OAIS is an organization of people and systems responsible for preserving information over the long-term and making it accessible to a specific class of users. Its high level repository structure diagram is reproduced in Fig. 1.

This reference model, now an international standard, identifies responsibilities that such an organization must address to be considered an *OAIS* repository. In order to discharge its responsibilities, a repository must:

- negotiate for and accept content from information producers;
- obtain sufficient content control, both legal and technical, to ensure long-term preservation;
- determine which people constitute the *designated community* for which its content should be made understandable and particularly helpful;
- follow documented policies and procedures for preserving the content against all reasonable contingencies, and for enabling its dissemination as authenticated copies of the original, or as traceable to the original; and
- make the preserved information available to the designated community, and possibly more broadly.

Almost every archive accepts these responsibilities, so that compliance is seldom an issue. However, the quality of compliance is often a matter of concern.

Fig. 1 tends to draw analysts' attention to activities inside repositories, in contrast to drawing attention to the properties of communicated information that are suggested by Fig. 2, which identifies the content transfer steps that must occur to consummate communication. Since the latter figure more completely suggests the potential information transformations that might impair the quality of communication than the former, we choose to focus on its view of digital object storage and delivery. A consequence is that our attention is drawn more to the structure of and operations on individual preservation objects¹⁵ than to the requirements and characteristics of digital repositories.

¹⁵ Schlatter 1994, *The Business Object Management System*.

Information transmission is likely to be asynchronous, with the producer depositing information representations in repositories from which consumers obtain it, possibly many years later. For current consumers, the producer might also transmit the information directly. The transfer will often be between machines of different hardware and software architectures. Producers cannot generally anticipate what technology consumers will use, or by which channels information objects will be transmitted, nor do they much care about such details.

Figure 2 helps us discuss preservation reliability and suggests that, in addition to requirements outlined in §1.2, thinking of digital preservation service as an extension of digital information interchange will make implementations rapid and inexpensive. For a comprehensive treatment, we must deal with the entire communication channel from each Fig. 2 producer's knowledge **0** to each eventual consumer's perceptions and judgments **10**, asking and answering the following questions.

- How can today's authors and editors ensure that eventual consumers can interpret information saved today, or use it as otherwise intended?
- What provenance and authenticity information will eventual consumers find useful?
- How can we make authenticity evidence sufficiently reliable, even for sensitive documents?
- How can we make the repository network robust, i.e., insensitive to failures and safe against the loss of the pattern that represents any particular information object?
- How can we motivate authors and editors to provide descriptive and evidentiary metadata as a by-product of their efforts, thereby shifting effort and cost from repository institutions?¹⁶

Kahn 1995, *A Framework for Distributed Digital Object Services*, <http://www.cnri.reston.va.us/home/cstr/arch/k-w.html>.

Maly 1999, *Smart Objects, Dumb Archives*.

Pulkowski 2000, *Intelligent Wrapping for Information Sources*.

Payette 2000, *Policy-Enforcing, Policy-Carrying Digital Objects*.

¹⁶ "... preservation in the digital age must be considered at the time of creation. Preservation cannot be an activity relegated to the expertise of libraries and archives, but rather must be seen as intrinsic to the act of creation."

NDIIPP Plan, p. 52

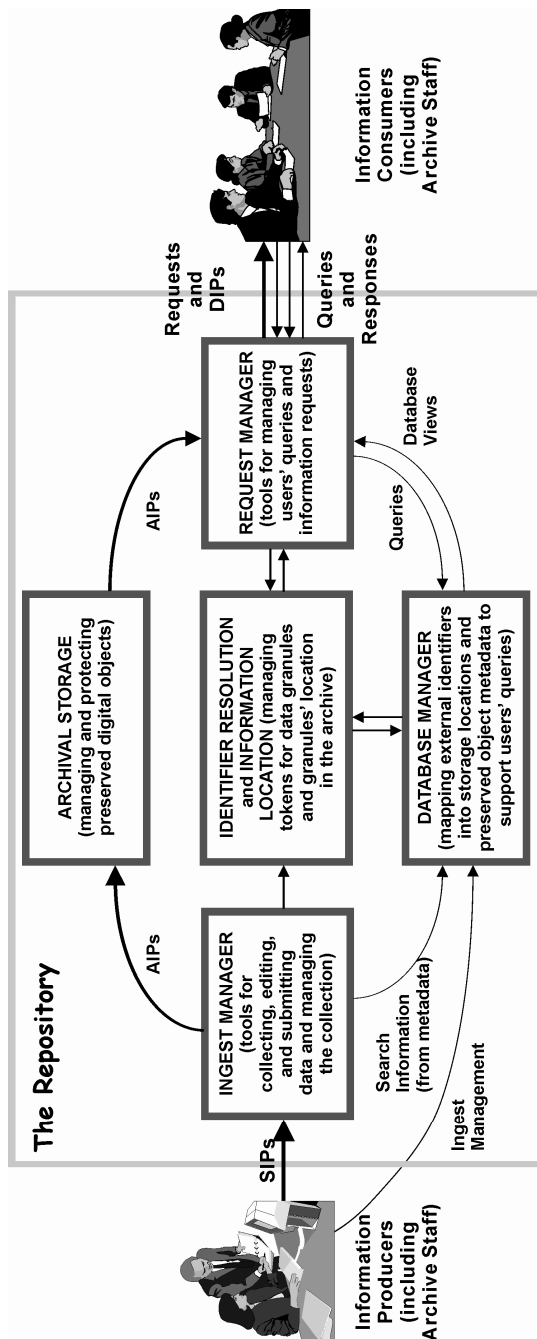


Fig. 1: OAIS high-level functional structure

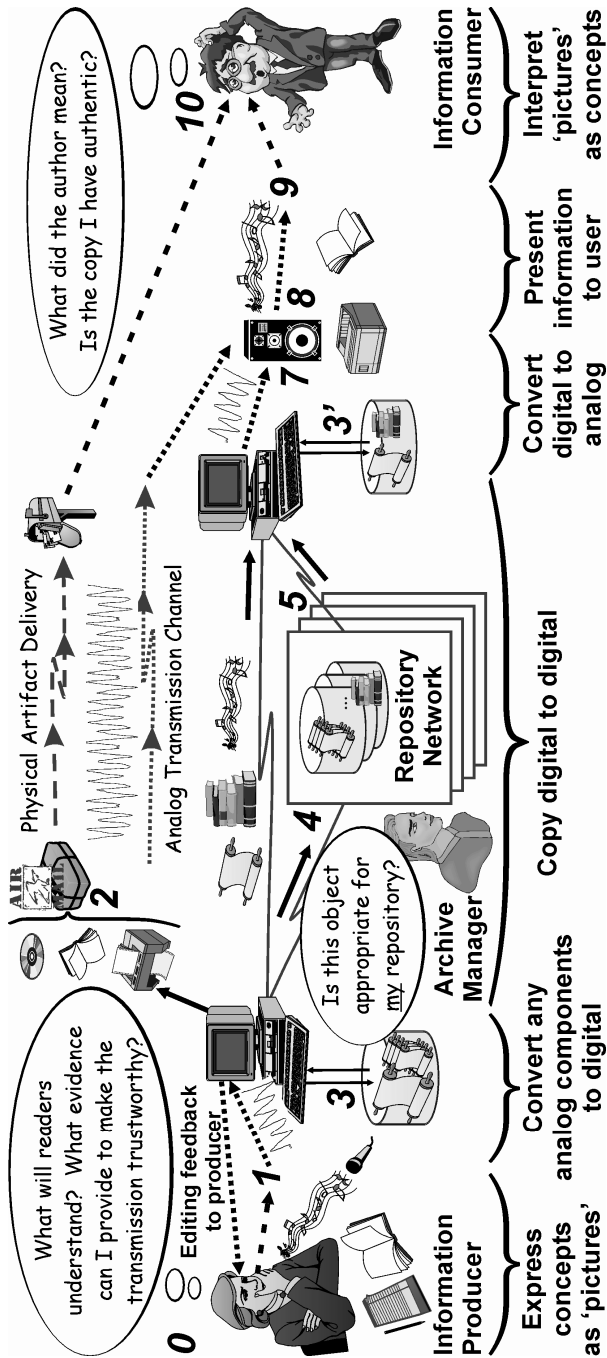


Fig. 2: Information interchange, repositories, and human challenges. The numerals name input and output objects. Some of these are ephemeral.

Of particular interest in Fig. 2 are the steps that include transformations that might impair communication integrity, as suggested in:

Table 3: Information transformation steps in communication

0 to 1	Create information to be communicated using human reasoning and knowledge to select what is to be communicated and how to represent it. This is a skillful process that is not well understood. ¹⁷
1 to 2	Encode human output to create artifacts (typically on paper) that can be stored in conventional libraries and can also be posted.
1 to 3	Encode analog input to create digital representations, using transformation rules that can be precisely described, together with their inevitable information losses, additions, and distortions.
3 to 4	Convert locally stored digital objects to what <i>OAIS</i> calls Submission Information Packages (SIPs).
4 to 5	Convert SIPs to <i>OAIS</i> Archival Information Packages (AIPs).
5 to 3'	Convert AIPs to <i>OAIS</i> Distribution Information Packages (DIPs).
3' to 7	Convert digital objects to analog forms that human beings can understand.
7 to 8	Print or play analog signals, with inevitable distortions that can be described statistically.
6 to 10	Convert information received into knowledge, a process called
9 to 10	learning and involving immense skills that are not well understood. ¹⁸

It will be important to persuade information originators to capture and describe their works partly because the number of works being produced is overwhelming library resources for capture, packaging, and bibliographic description. It is particularly important because originators know more about their works than anyone else. However, this is offset by the fact that they rarely will be familiar with cataloging and metadata conventions and practices—a problem that might be mitigated by providing semiautomatic tools for these process steps.

Digital capture close to the information generation is especially important for performance data in entertainment and the fine arts, because only producers can capture broadcast output without encountering both copyright barriers and signal degradation. Consider a television broadcast created partly from ephemeral source data collected and linked by data-dependent or human decisions that are not recorded but exist implicitly in the performance itself. Ideally, capturing performances for preservation can be accomplished as a production side effect. More generally, nontech-

¹⁷ Ryle 1949, *The Concept of Mind*, Chapter II.

¹⁸ Ibid., Chapter IX.

nical barriers embedded in the channels that connect data sources with a public performance might impede what would be best practice in ideal circumstances.

1.5 Technical Objectives and Scope Limitations

Technology informs almost every aspect of long-term preservation. It is not widely believed that ... solutions can be achieved solely through technological means. ... there is consensus around the following challenges: media and signal degradation; hardware and software obsolescence; volume of information ... urgency because of imminent loss; and ...

NDIIPP, Appendix 1, p.4

The *Open Archival Information Systems (OAIS) Reference Model* and related expositions address the question, “What architecture should we use for a digital repository?” This includes all aspects of providing digital library or archive services, including all important management aspects: management of people, management of resources, organization of institutional processes, selection of collection holdings, and protection against threats to the integrity of collections or quality of client services. Among the threats to collections are the deleterious effects of technology obsolescence and of fading human recollection. Efforts to mitigate these information integrity threats make up only a small fraction of what library and archive managers need to plan and budget for.

In contrast to the *OAIS* question, *Preserving Digital Information* asks a different question, “What characteristics will make saved digital objects useful into the indefinite future?” Such different questions of course have different answers.

Of the several dimensions of digital preservation suggested by the long quotation in §1.1, this book will focus on the technical aspects. We construe the word ‘technical’ as including clerically executed procedures, just as the word ‘technique’ spans mechanical and human procedures. Many topics that might appear in a more complete prescription of digital archiving have been thoroughly treated in readily available information technology literature. For such archiving topics, this book is limited to short descriptions that position them among other preservation topics, to relating new technology to widely deployed technology, and to the identification of instructive sources. For instance, digital library requirements and design are discussed only enough to provide context for changes that preservation requirements might induce.

The book is intended to suggest only document management aspects required for preservation, without getting involved with whatever mechanisms people might choose to manage related needs, and without com-

menting on proposals for satisfying such needs. It avoids most aspects of collection management, most aspects of librarianship, and most aspects of knowledge management. Such restraint not only avoids distracting complexity, but also tends to make the book's preservation recommendations architecturally compatible with installed software for these avoided areas, as well as with most of the literature discussing the other topics.

The book is motivated by the exponentially growing number of "born digital" documents that are mostly not tended by society's libraries and archives. Its technical measures of course extend without modification to works digitized from their traditional predecessors, such as books on paper. They are particularly pertinent to audio/visual archives. However, since the technology needed to maintain analog recordings is already well handled, we include it only by reference (§7.2.4).

Some topics to which the practitioner needs ready access are so well and voluminously described that the current work limits itself to identifying sources, discussing their relationships to the underlying fundamentals and their pertinence to digital preservation, and suggesting source works of good quality. Such topics are XML, with its many specialized dialects and tools, information retrieval, content management of large collections for large numbers of users, and digital security technology. Other prominent topics, such as intellectual property rights management and copyright compliance, are not made significantly more difficult by adding preservation to other digital content management requirements,¹⁹ and are therefore treated only cursorily.

The solution, which we call Trustworthy Digital Object (TDO) methodology, addresses only the portions of the challenge that are amenable to technical measures. Of course, to accomplish this we must clearly distinguish what technology can address from what must be left for human skills, judgements, and taste. For instance, we do not know how to ensure that any entity is trusted, but do know many measures that will allow it to advertise itself as being trustworthy, and to be plausible when it does so. Thus, *Preserving Digital Information* must include an analysis of philosophic distinctions, such as that between trusted and trustworthy, in order to provide a good foundation for justifying the correctness and optimality of TDO methodology.

Many published difficulties with what is required for long-term digital preservation are digital content management issues that would exist even if material carriers, digital hardware, and computer programs had unbounded practical lifetimes. This book therefore separates, as much as possible, considerations of durable document structure, of digital collection man-

¹⁹ Gladney 2000, *Digital Intellectual Property: Controversial and International Aspects*.

agement, and of repository management. It says little about internal repository workings that relate eventual outputs to histories of inputs, but instead treats repositories as black boxes whose interior mechanisms are private to the staffs of repository institutions. This approach has the desirable side-effect that we minimize meddling in other people's business.

1.6 Summary

Digital preservation is critical to most of the history of the future.²⁰ This justifies every practical effort to ensure that the technical methodology used to accomplish it is sound and widely understood.

As business, government, and cultural records migrate from paper to digital media, the importance of digital archives will increase. Enterprises considering creating and managing repositories know that a document might be important five to 100 years later, and that technical obsolescence might by then make it irretrievable in any meaningful way. For instance, pharmaceutical development records must be held until the risk of lawsuits subsides many years after the drugs are sold. Doing this safely and inexpensively is not general practice today.

Consideration of the reliability of information on which we depend must include recognition that deceit can permeate agendas and transactions and that information flows so rapidly and in such great quantities that human errors are inevitable. Even if we had the resources to examine each saved record carefully, we would find it difficult or impossible to predict how it might be used and what risks its user might incur. Such circumstances motivate a strategy to protect all objects as if they were targets of attacks that destroy their integrity. A solution that is inexpensive in the document preparation needed for preservation, possibly with significant costs limited to the small fraction of objects that their eventual users decide to test, would be economical for all preserved data objects. Happily, such a solution exists (Chapter 11) and can be implemented to be an almost automatic side effect of saving documents that are being edited, or opening preserved documents for viewing.

We emphasize end user needs—what people acting in well-defined roles might need or want to accomplish specific tasks, rather than emphasizing how repositories might work. Preservation can be viewed as a special case of information sharing. It is special because consumers cannot obtain producers' responses for puzzling aspects or missing information.

²⁰ Cullen 2000, *Authenticity in a Digital Environment*, <http://www.clir.org/pubs/reports/pub92/cullen.html>.

Digital preservation is a different topic than repository management. The distinction is made particularly clearly in the program of the National Archives of Australia, which partitions its system into three components that share documents only by transported storage media: a quarantine server, a preservation server, and a digital repository.²¹

The book is limited to technical aspects of preservation, leaving social and managerial aspects of repositories and more general document management to other authors. It discusses digital repository design only to the extent necessary to provide preservation context—the technical infrastructure into which preservation software must be integrated.

Throughout, the book's focus is directed toward methods for preserving each intellectual work, leaving the management of repositories and social factors, such as training of archival personnel, to other treatments. The key novel challenges are:

- ensuring that a copy of every preserved document survives “forever”;
- ensuring that any consumer can decide whether or not to trust a preserved document; and
- ensuring that consumers can use any preserved document as its authors intended.

²¹ Wilson 2003, *Access Across Time: How the NAA Preserves Digital Records*, <http://www.erpanet.org/events/2003/rome/presentations/Wilson.ppt>.



<http://www.springer.com/978-3-540-37886-0>

Preserving Digital Information

Gladney, H.

2007, XXIII, 319 p., Hardcover

ISBN: 978-3-540-37886-0