SECTION I

The Problem

CHAPTER ONE

Archival Data Management to Achieve Organizational Accountability for Electronic Records

CHAPTER TWO

Recordkeeping Systems

CHAPTER ONE

Archival Data Management to Achieve Organizational Accountability for Electronic Records*

Organizations which adopt digital means of communication need to be much more alert to issues of data management throughout the life cycle of records in order to ensure accountability. Requirements for records management and archives need to be made much more explicit than they have traditionally been. Tactics which are available need to be selected based on careful analysis of the organizational culture and technical capabilities. Conscious risk management decisions will need to be made at the highest levels of the organization around numerous decisions affecting records creation, retention, and access. Overall, the electronic office environment will force organizations to view archives in a new light and to change organizational behavior with respect to recordkeeping or lose the ability to reconstruct or defend their past behavior. Archivists will find the demands of data management in electronic records environments force them to reaffirm their most fundamental theoretical tenets, rather than to reject them as they have often feared.

* Originally published in *Archives and Manuscripts* 21:1 (1993): 14-28.

INTRODUCTION

Archives and records management share a simple goal: providing for organizational accountability. However achieving this goal in the era of electronic information systems is far from simple. Accountability depends on being able to demonstrate managed access to information which is important for reasons of ongoing need or future evidence, from the time of its creation. In the public sector accountability must protect privacy at the same time that it ensures the public right to information about the operation of their government. To provide such continued and accountable access, organizations are struggling to redefine archival programs in order to document and preserve the information content, structure, and context of the electronic evidence of activity they undertake as part of their missions.[1]

Articulating and communicating these requirements to program administrators and to data processing or systems managers is a critical archival role. It will only bear fruit when the staff throughout the organization understand the nature of electronic records and the importance of records of business applications in which they participate to accountability. This chapter begins by examining ways of explaining why electronic records present a challenge to organizational accountability and how to articulate archival functional requirements.

Records managers and archivists focus their strategies on application systems, both because business applications generate records and because the specific requirements for retention of evidence arise from the nature of the transactions which characterize different business functions. Once focused on business applications, records managers and archivists can assess the possible tactical approaches to ensuring control over evidence until it is acceptable to discard it. Specific approaches are examined in the third section of this chapter.

Risk management methodologies can help to support their decisions. Risk management approaches place archives

and records decisions in a more appropriate context than do cost/benefit approaches. While long-term benefits are largely inestimable, risk assessment is appreciated by experienced managers who use it to estimate the probability of a variety of outcomes.

Because the risks that must be managed by archivists and records managers arise throughout the life cycle of electronic information systems, their control requires continuity of rigorous data management practices. These data management practices are equally applicable to vital records management, privacy, freedom of information, and security. Archivists will find an increasing need to exploit these interests in common with other organizational functions in order to achieve their missions. In addition, they will need to understand the areas of continuity and discontinuity in their own practices that have been introduced by new electronic communications environments.

DEFINING THE PROBLEM

Methods of communication within organizations are being rapidly, and radically, transformed as a consequence of the introduction of electronic, computer-based, communications technologies. It is now becoming evident that these technologies are not just providing a new method for transmission of information but changing the social character of the communication. Instead of compiling an analytic report or sending a reasoned letter to the appropriate corporate authority (and expecting after an interval to receive an equally well researched and reasoned reply), electronic communications encourage an interactive, dialogue-like, interaction. In this dialogue, brief sorties to the database extract further clues and these are passed along in a relatively undigested form. As the character of the interchange is altered, so are the "forms" of the documentary record.[2]

In the world of paper records, we know that particular "forms" are associated with interchanges that have specific

functions. For example, archivists and records managers can identify generic forms which will be involved in any governmental service delivery function. These functions will involve transactions in which clients are registered, in which needs are documented, and in which contact histories are kept. Archivists and records managers use their knowledge of the relationships between functions and forms of documentation to "schedule" records or determine how long the information in each needs to be kept. They are able to make these decisions on the basis of the form of the record and the function that created it without looking at concrete instances of these records. Any organization can identify "forms" specific to particular business transactions in which it engages. Data management guidelines will be specific to each form because records need to be kept a given length of time as a consequence of the character of the transaction about which they are evidence, not because of the specific information that may or may not be in them or because of who sent or received them.

The communication environment into which we are now moving is one in which electronic information systems will soon be ubiquitous and communications between persons in and outside of an organization will take place electronically. In addition to altering the "forms" of records, electronic systems erode the basic boundaries used by archives in making their judgments. The location of records storage will increasingly become arbitrary as will the "original order" of the file. With the loss of these landmarks, archivists will be forced to redefine their requirements for managing records. In such an environment archivists and records managers need to have criteria for determining what is a record and tactics for capturing them. Because records are evidence of business transactions, they will always be communicated across a physical or logical communications switch in an electronic system. After all, they can hardly serve as communications unless they are sent. If archivists can define which messages from what transactions are to be captured as records, they can save them.

How well archivists are able to ensure the preservation of evidence will depend on the tactics they employ to enforce good data management practices. However, the fact that different corporate cultures have very different climates for electronic records management and that the variables in corporate culture which influence the success of tactics employing policy, design, implementation procedures, and standards are not yet known. This is still a hit-or-miss proposition.[3]

ARCHIVAL FUNCTIONAL REQUIREMENTS

In 1989 the author was contracted by the United National Administrative Coordinating Committee on Information Systems (ACCIS) to recommend policy guidelines for the management of electronic records.[4] The first step in defining necessary policy guidelines, or necessary systems design, implementation, or standards requirements, is to establish functional requirements for electronic records management. If we could agree on such requirements, we could define policy approaches as well as other approaches to satisfying them.[5]

Nine functional requirements were identified which emerged from three broad areas of concern: (1) the need to identify electronic records within the organization; (2) the need to assign responsibility for administering them; and (3) the need to establish controls that will satisfy accountability and take into consideration the technical nature of electronic records.

The first three functional requirements concern the identification of electronic records, including the identification of electronic records, including defining their essential characteristics and establishing means for retaining them.

(1) Archives must be able to identify electronic records.

We must know what data comprises a record and what is not, and we must know why in terms that can be implemented in, through, by, or around information systems. In the policy

guideline we asked "Does policy define the concept of record and non-record electronic information in a way that can be implemented by people and systems?" In discussion of the guidelines and in work which has followed, the author has depended on a definition of records as business transactions. That is records are transactions which have a significance in business terms (rather than in computing terms) because they constitute evidence of a business event, such as making a sale or qualifying a client to receive a benefit. A functional requirement of corporate accountability is: (a) that any such business transaction must create a record, and (b) that archivists must have a business rule for how long and for whom to retain the records and when and for whom to provide for their use.

(2) The organization must decide what to do with its records and why.

As I put it in the UN ACCIS report, archivists must be able to "articulate criteria for retention that will yield acceptable results for electronic records and be consistent with those for eye-readable records even if the results of applying such criteria are different." Archivists and records managers have historically employed implementation-based strategies to ensure application of retention criteria. In effect, we said that organizations will file like materials together because this corresponds to the way they do business, and that as a consequence we can schedule (determine the appropriate disposition for) records without looking at individual items but only at "series." In electronic systems, where physical storage is random and cannot guide us to like records, and logical organization permits many different, overlapping "views" to exist at the same time, the series corresponds to the records of one type of business transaction. For this reason it is clearer that what we are appraising is the need to retain records of a business transaction which is in turn based on a combination of legal requirements, known needs for the records, and calculated risks associated with their destruction. This appraisal can take

place before any records are actually created and can be applied without actually looking at any records which result from the process, because the criterion is evidence, not information. Each type of business transaction has an accountability requirement of which the records retention decision is simply a reflection.

(3) Records retention determinations must be executed in a timely fashion.

Again this can be achieved through policy, design, implementation, or standards, and depends only on the unequivocal ability to define when records are no longer needed. While this is usually done with paper records in an extremely simple way, by defining a fixed date for destruction, relative destruction dates and retention for "continuing value" have been much harder to implement in traditional systems than they will be in electronic archives. Because records will be identified as "archival" in the electronic environment from before the moment of their creation the concept of "timely" scheduling becomes superfluous.

The first three requirements spoke to identification of electronic records in the organization. The next three are, broadly speaking, administrative.

(4) No organization can expend more effort or money on managing records and archives than can be justified by the risks it would run or the benefits it would forego if these efforts were not invested.

Criteria must be established to measure program success and to ensure that investments in electronic records management are effective. The fourth section of this chapter identifies numerous generic risks, but organizations need to define their own risks and levels of risk acceptance. Archivists have a role to play in identifying sources of risk and criteria for evaluation based on archival functional requirements.

(5) Appropriate administrative units must be assigned explicit responsibilities in the management of electronic records.

These responsibilities must be defined in a concrete and measurable way and include minimally:

- the articulation of each business application's requirement for evidence,
- the formulation of specifications or system evaluation methods,
- testing the ability of the system to satisfy the requirements,
- educating users in system functions and the risks they avoid,
- establishing data management guidelines and audit plans,
- defining metadata and documentation requirements for data, structure, and context,
- conducting ongoing technology risk assessments,
- developing migration plans that ensure migration of evidence rather than just information, and
- defining access methods for users.

(6) Organizations must decide where, and under whose control, electronic records should reside over time.

Because physical custody of electronic records does not ensure their evidential integrity unless they are defended by other security barriers, the day-to-day data management responsibilities must be assigned to the offices which create and manage the content of the records rather than to an office which has physical control. Intellectual control can be maintained for records which are not in physical (or even legal) custody, but in electronic systems it is difficult to ensure the accuracy of such controls unless they are actively linked to the records.[6] This is frequently where the policies break down.

Archivists are accustomed to demanding physical custody even though they are less well equipped to take on this responsibility than the office in which the records system is currently maintained. In addition, the costs to the organization are likely to be considerably higher because migration of the archival records will need to take place independently from migration of current records.[7]

The seventh through ninth functional requirements address integrity. In each of these areas the organization must act to safeguard the continuity of the evidence it has identified and captured. Failure to establish and maintain systems which appropriately address these requirements abandons the record.

7) The legality of the electronic record must be safeguarded, e.g., it must retain its unequivocal connection to the action of which it is evidence.

The direct analog of this issue, the admissibility of microform in place of original records in courts has long been a feature of archival practice and of the laws of evidence. The criterion which ultimately determines admissibility is continuity of management. If we can demonstrate that normal business practices were implemented and followed, the microform will typically be accepted as best available evidence where no original exists. With respect to electronic records, the concept of managing the data environment to protect the evidential quality of documentation arising from continued and protected custody, becomes critical. Data management practices and procedures, and evidence from audits and observation of their general implementation, will be the best way to preserve the legality of electronic records as evidence.

8) Related data management issues of security, privacy, confidentiality, and, in government settings, freedom of information must be addressed.

Each of these policy concerns requires the same level of data management control as archives and typically needs to be exercised at the same time and in the same ways as for

archives. By identifying each of these policy issues up front in systems planning, design, and implementation, similar approaches can be taken to ensure their achievement.

9) The hardware, software, storage media, and documentation techniques must be evaluated to ensure that the records will indeed be preserved and remain usable over time.

Electronic records are always virtual documents, that is they exist under software control and are dependent on some hardware, even if they are (someday) truly "inter-operable" across hardware platforms. Because a generation of hardware and software (the length of time before obsolescence) is less than five years and because storage media generations are equally volatile, the electronic records must be regularly migrated to new hardware, software, and media. How frequently such migrations must occur will depend on how good the decisions about previous migrations have been. How valid the results of any given migration, or of the entire history of movements, will depend on documentation. Documentation also determines whether we can demonstrate the reliability of migrated records as evidence.

Failure to satisfy the functional requirements concerning access renders the entire endeavor purposeless. Here any successful approach must prevent the media and format of records from being barriers to accessing them, and it must establish standards for intellectual control and documentation that rise above the software-dependent norms. For any given records, we must also determine what, if any, functionality of the system must be preserved as evidence, and how to do that.[8] Even if functionality is unnecessary, the program must still dictate how contextual data is to be retained in a usable form so that it will be clear how the record could have been used and would have been seen by those who were conducting the business at the time of its creation.

The organization must also address the basic issues about access that are present for any records, such as who is to be

given access and what uses they will be permitted to make of records which they have seen. Archivists must recognize that in electronic environments these issues play themselves out in systems design and implementation, bear on functionality, and must be managed continuously. While in paper environments access is external to the record system, electronic records are accessed through the system. While paper records can hardly be used at all except in their entirety, it is easy to provide partial access to electronic records, indeed preserving the users' view of a database for future research is a matter of masking some data and functionality while exposing other data and manipulation capabilities.

TACTICS

Four tactics (policy, design, implementation, and standards) have been identified as having potential for the accountable management of electronic records. It is essential for us to examine these four approaches to satisfying archival requirements in greater detail in order to develop tactics appropriate to each other.[9]

Policy, both at a general level and in its more detailed form as procedure, provides guidelines for how people should use electronic information systems. By identifying the various needs which the organization has for evidence from electronic information systems, policy can in principle provide instructions to people about how to ensure the creation and retention of such evidence. In most corporate cultures, however, policy will not alone provide adequate assurance that electronic records are created and managed appropriately.

As a result, archivists over the past decade have stressed systems *design* and up front involvement by archivists in the specification of systems as a more certain means of ensuring satisfaction of archival functional requirements.[10] However, design-based approaches have drawbacks: they can be quite expensive, they can defeat the operational functional requirements, and they can depend on archivists being able to specify

precisely what systems need to do in order to meet archival needs. In addition, the best designed systems can be defeated by poor training of staff or incomplete or insensitive implementation.

Therefore, *implementation* has also been identified as an approach to satisfying archival requirements in electronic information systems. Providing guidelines for appropriate implementation of systems is not overly complex, but getting the users and the data processing support staff to understand the requirements, without which they will fail to realize the implementation objectives, can be very difficult. Like policy, implementation guidelines may not be applicable in some corporate cultures or with certain business applications. Especially in very routine applications, it may be necessary to depend on external information technology standards to achieve long-term compliance.

Information technology (IT) *standards* have long been attractive to archivists confronted with the problems of electronic records because they appear to be a magic bullet. It is as if we said "If we could make archival functional requirements part of an international IT standard then all systems would automatically meet them." Unfortunately, however, archival functional requirements have not been explicitly articulated and one of the few which has been, e.g., software interoperability, has also been the ultimate goal of IT standards developers for the past decade and is still very far out of reach.

RISK MANAGEMENT

Choosing tactics and defining practical standards for satisfying the functional requirements for electronic archives in the real world involves identifying and judging risks. Organizations have to understand the risks posed by the social requirement of accountability. For public organizations the ultimate risk is the loss of legitimacy and for private organizations it is incurring liabilities beyond the capacity of the organizational purse. Public and private organizations must,

therefore, adopt methods for managing the risks created by documentation and its absence just as they adopt strategies for dealing with risks such as changing interest rates, product liability, or employee malfeasance. In fact, the tactics for managing these archival risks can best be tested using methods derived from the experience organizations have in self-insurance, managing financial risks, or managing risks associated with political decisions.

These risks include, but are hardly limited to:

- failure to locate evidence that an organization did something it was supposed to have done under contract or according to regulation,
- inability to find information that is critical for current decision making,
- loss of proof of ownership, obligations owed and due, or liabilities,
- failure to document what the organization knew at the time of an important transaction, and hence whether it behaved according to its own policies or in adherence to law,
- inability to locate in the proper context information which would be incriminating in one context but innocent in another,
- inability to demonstrate a pattern of documentation providing evidence that policies and procedures in effect in the organization were responsibly followed.

These risks are particularly great when employees in the organization do not recognize that records are, or should be, created, as a consequence of transactions. Electronic communications are not uniformly regarded as having the same significance as communications on paper, but are sometimes seen as more analogous to verbal commitments even though the organization will in fact be held liable for them. As a result employees will fail to create records at these junctures or will not require their systems to be designed so as to ensure such record creation. Indeed the concept that what the employee

sees on his or her screen may not "actually exist" except on that screen and have no existence as a record is not something that we have successfully communicated even to management. Risk may arise because employees do not see themselves as accountable through records for their actions over time, but a more likely cause is that the concepts of records which employees are trained to use have no analogs in the electronic systems being implemented. If we fail to provide employees with concrete examples of the new risks they are incurring or of new definitions of records, they can hardly be considered individually culpable for overlooking necessary steps in documenting activity. The underlying problem is that employees are not given assistance to modify their own behavior. Organizational requirements for evidence are not explicit or are unknown to those who create and manage records. In the past organizational requirements would probably be satisfied if records were kept as a consequence of forgetfulness. Guidelines for disposition did not need to be well known.

Passive retention will not be adequate in the future however because unless serious attention is paid to data management throughout the life of the record, organizational records will not be created, be retained, or be acceptable as evidence. Now that electronic records show no traces of the changes they have been subjected to unless the system requires such traces to be left, methods for data management throughout the life of a record are critical and cannot be inadequately documented, inadequately followed, or inconsistently applied. Without systematic data management, it cannot be demonstrated that organizational records were not altered over time by purposive intervention or unconscious change introduced during migrations.

In addition to the risk of loss of evidential value, the organization runs a risk of losing even the use value of the information records contain. Often, organizational records in electronic form cannot be related to paper records from the same business transactions which are retained in mixed media

archives. Frequently organizational records in electronic form cannot be read, retrieved, decoded, or accessed because they are too fragile, too poorly documented, the software to decode them is unavailable, or the context of their creation and use cannot be reconstructed to give them meaning. Over time the organization may find that its records cannot be invested with the functionality they had in the environment in which they were used and that this functionality is crucial to understanding them. Because records have not been segregated by retention, the organization may find that it can no longer afford to keep all it has nor develop techniques for identifying levels of risk that would permit it to select from among what it has kept. Finally, records which contain information that must be protected for reasons of confidentiality, security, proprietary and other restrictions may not be identified, and as a consequence the organization cannot allow access to any records because their restricted content cannot be separated without the cost of having human beings read through all records with these criteria in mind.

This array of risks can be minimized through planning grounded in risk management. First it requires that senior management define the risks associated with records and make everyone in the organization aware of these risks, of the steps being taken to contain them, and of the penalties which the organization will impose on those who fail to support accountability. Second, management must adopt risk management criteria for program effectiveness and enforce data policy requirements including security, privacy, vital records recovery, freedom of information, and archival preservation. And the organization must implement systems with conscious regard for limits of interoperability, especially with sensitivity to access requirements as the source of media standards.

Management and staff must understand the risks inherent in electronic records. First, electronic records are software- and hardware-dependent to some degree, regardless of standards, because records exist only under software control. What actu-

ally existed for the person using or receiving an electronic record is not easy to replicate or document because of the many layers of software through which it is mediated. While in most situations these niceties may not matter a great deal, they do mean that it is exceptionally difficult to retain the actual evidence of a transaction and that the organization runs a significant risk of retaining something which can be argued not to be evidence.

Even if evidence can be kept, the organization runs a substantial risk that continuing access costs are unpredictable even over relatively short periods, to say nothing of the potential cost of "permanent" records. With rapidly changing hardware and software environments, maintaining systems longer than their supported life is dangerous and migrating data and software functions is complex and equally costly. If programmers are going to reconstruct the data to map it to new systems during migration, they need to have the ability to alter the information structure, and often its contents, during the process.

Information content is independent of systems design, but evidence is design dependent. Therefore, even what is maintained may be modified (if inadvertently) by redesign of the system holding it. Such losses of evidential value as a consequence of redesign are extremely difficult to detect. In addition, the actual data content is subject to alteration during the migration because it is not possible to redesign and migrate data in an environment that is sufficiently controlled that we could say without hesitation that no alterations could have been made to the records or that the resulting system operates in all respects like the previous one. Finally, even if the migration maintains absolute fidelity to evidence and functionality, the new system might be perceived by users as different because "records" in electronic information systems are mediated by users' mental models and we understand little about how such models come to be. As such we are unlikely to create the

"same" system from a user's point of view when we migrate electronic records.

Despite these risks, the best framework we can provide for access involves: (1) continuing migration as solution to permanence standards; (2) metadata as the mechanism of intellectual control; (3) migration of functionality, contextual documentation and configuration management as strategies for retention of information context; and (4) an Information Resource Directory System (IRDS) as the directory for remote access.

IMPLICATIONS FOR ARCHIVAL PRACTICE

Despite the seemingly alien aspects of electronic records management, there are large areas of continuity with traditional archival practices. To begin with, the fundamental principle of archival practice, its traditional emphasis on "respect des fonds," "provenance," and "original order" reflect evidential value of context of creation and use. In electronic records management these principles are of even greater importance since randomly stored data are otherwise devoid of context and only knowledge of the business application, or provenance, of the system provides guidance for retention.[11]

As with traditional records, the appraisal of electronic records is based on series, rather than items, so that with proper design, electronic records with common content can be identified and controlled. The concept of a series has less of a physical referent with respect to electronic systems, emphasizing instead the relationship between "form" of records and the character of the specific business transaction. As a consequence it is more evident that it is the evidence of a certain transaction which is appraised rather than the records, and hence appraisal can and does take place without records having yet been created.

And while the tendency is admittedly more pronounced with electronic records, there is increasing decentralization of recordkeeping and, therefore, of responsibility for manage-

ment of organizational memory even in traditional settings and with paper-based systems. Distribution of records creation and management implies that policy adherence depends on understanding of records management requirements by program staff and their ability to use the installed information systems to achieve the objectives of maintaining information quality (integrity, currency, and relevancy) and continuity of access. De facto standards are unlikely to be effective means of ensuring interchangeability of information because system implementations and upgrades will occur at irregular times and in an uncoordinated fashion throughout the institution. Directories bridging distributed files will be essential for stored information to be retrieved.

Of course there are areas of discontinuity as well. The most important and difficult to grasp is that traditional records are created and stabilized on a medium in a single act, thus the record is necessarily evidence of the act. Electronic information systems do not necessarily create or fix evidence of acts, and are designed to be "efficient" by reusing the information content of the system many times, without leaving a trace of its prior state unless systems was designed to document record transactions.

In traditional environments, appraisal is conducted at time of accessioning, and therefore appears to be an assessment of the records themselves. In electronic records management, initial appraisal must take place at the time of system design or before and is therefore more obviously a reflection of the function. Traditional appraisal tends to occur once, based on determination of permanent value, while electronic records management requires focus on continuing value because risk factors change with each system migration.

Because the costs of retaining traditional records are much greater if they are distributed, paper records are typically transferred to central archives. Different cost and risk factors dictate that electronic records be managed within the originating context as long as possible. The difference in outcomes

here mask the application of a common criterion, but to most archivists it seems a radical difference.

A similar difference in outcomes reflecting application of a common standard applies to preservation. Traditionally preservation of the medium has been the focus, but in electronic records management, preservation of usable access to information will not be assured by media preservation alone. Hence emphasis is shifted to the information. But in the traditional setting, the preservation of the medium assured continuing access to the information, so there may be no conflict of intention.

Indeed this seems likely when we examine differences directly associated with access. Traditionally users come to records and find information they require because this is the only way it can reasonably be made available to them. In electronic records management the concrete information required can be delivered to remote users by request and in configurations best designed to be usable for their purposes (based on their use of metadata to formulate an inquiry). The costs of making information in electronic form available to the user at his or her site may, in fact, be less than the cost of maintaining a central reference space for such users and the convenience to the users is far greater.

NOTES

[1] David Bearman, "New Models for Management of Electronic Records by Archives," *Cadernos de Biblioteconomia, Arquivística, e Documentação* 2 (1992): 61-70, reprinted in this volume as Chapter 10.

[2] David Bearman and Peter Sigmond, "Explorations of Form of Material Authority Files by Dutch Archivists," *American Archivist* 50 (Spring 1987): 249-253. "Form" is an abstraction of something we recognize culturally but for which we do not have a generally accepted or named concept. Indeed, most people will need to have the concept illustrated (a receipt, a memo, a classified ad, or an application are each a form because we would recognize them even if the words were changed to xxxx's). Yet once they understand the concept it is clear to people both that recognition of a 'form' is a significant part of "literacy" and that electronic information interchange has yet to evolve recognizable 'forms' and that this contributes to the difficulty we have in managing it.

[3] The archives and records management community needs a study of a variety of business application areas, in different firms, with case analysis of the degree of success encountered in implementing solutions to records management problems using combinations of four approaches to satisfying the same set of functional requirements: policy, design, implementation and standards. A large scale interdisciplinary study along these lines was funded by the National Historical Publications and Records Commission to be conducted at the University of Pittsburgh, beginning in 1993.

[4] David Bearman, "Management of Electronic Records: Issues and Guidelines," in United Nations Advisory Committee for Coordination of Information Systems, *Electronic Records Management Guidelines: A Manual for Policy Development and Implementation* (New York: United Nations, 1990), 17-70, 89-107, 135-189.

[5] These functional requirements represented my first private effort to think systematically about this approach to specifying how archives need to work. In the spring of 1993, with funding from the NHPRC, we were able to bring together a group of experts to address these questions collectively. Their definition of functional requirements is reprinted in Chapter 2 of this volume in Figure 2.7. Since then the functional requirements have undergone further refinement and revision, as reflected in the spring 1993 version printed in Appendix A of this volume. While further modifications are likely, the current re-

quirements all have substantial literary warrants and are unlikely to be significantly altered.

[6] Links or pointers from one database system to another are increasingly being employed to reduce redundancy and ensure the accuracy of data, but their effect is to change documents and views over time, thereby eliminating the value of a record as evidence. In addition, the assumption in any such live link is that the thing pointed to will still be available, physically and logically, to the pointing system. This assumption becomes increasingly invalid over time, leaving records as mere shells consisting of pointers to non-existence data.

[7] David Bearman, "An Indefensible Bastion," in David Bearman, ed., *Management of Electronic Records*, Archives and Museum Informatics Technical Report #13 (Pittsburgh: Archives and Museum Informatics, 1991): 14-24.

[8] The functionality of an application system is, of course, directly correlated with the work process it is intended to support. In order to understand what records meant and how they could have been used in the office which created them, it is essential to be able to understand the application environment. As an example, we cannot use a manual record system in which the two series are arranged by date of transfer and by lot number to search for property owned by John Jones. The files we are looking in cannot reasonably be employed in this way unless the user has first gone to the taxation bureau and found, in a series arranged by taxpayer name under John Jones, the lot numbers for the properties on which he paid taxes.

[9] David Bearman, "Archival Principles and the Electronic Office," *Information Handling in Offices and Archives*, Proceedings of a Symposium on the Impact of Information Technologies on Information Handling in Offices and Archives, Marburg, Germany, 17-19 October 1991 (New York: K.G. Saur, 1993), 177-193, reprinted in this volume as Chapter 5; also Bearman, "Diplomatics, Weberian Bureaucracy, and the Management of Electronic Records in Europe and America," *American Archivist* 55 (Winter 1992): 168-180.

[10] David Bearman, "Information Technology Standards and Archives," *Janus* (1992.2): 161-166, reprinted in this volume as Chapter 7.

[11] However, it is clear from our exposure to electronic records that the provenance of records is not equivalent to the "office of origin" but rather the function which gave rise to them, or more specifically the transaction within the function. For recent reflections of this re-

newed emphasis on function in description, appraisal, and archival education, see: Margaret Hedstrom, "Descriptive Practices for Electronic Records: Deciding What is Essential and Imagining what is Possible," paper given at the Association of Canadian Archivists Annual Meeting, Montreal 1992; Angelika Menne-Haritz, "Archival Education: Meeting the Needs of Society in the Twenty-First Century," paper delivered at the 12th International Congress on Archives, Montreal 1992; Helen Willa Samuels, *Varsity Letters* (Metuchen, New Jersey: Scarecrow Press, 1992).