Building Record-Keeping Systems: Archivists Are Not Alone on the Wild Frontier

MARGARET HEDSTROM*

RÉSUMÉ Des recherches récentes dans le domaine des documents électroniques ont mis de l'avant des propositions et établi des modèles en vue d'inclure des fonctions et des procédures de contrôle de l'information au sein de systèmes informatiques pour s'assurer de l'authenticité et de l'intégrité des documents. Cet article passe en revue plusieurs projets de gestion des documents informatiques menés par des archivistes et examine ensuite des progrès récents en matière de sécurité des réseaux et d'authentification sur la base des recherches réalisées à l'extérieur de la communauté archivistique. Mettant l'accent principalement sur le développement de « systèmes sécurisés » (*trusted systems*) destinés à soutenir le commerce électronique et la publication numérique, l'article évalue diverses méthodologies alternatives offrant des solutions partielles aux préoccupations en matière de gestion des documents informatiques. Il montre en quoi les méthodologies employées pour le développement de systèmes sécurisés sont compatibles avec les objectifs archivistiques et soulève certaines préoccupations en matière de préservation et d'accessibilité à long terme.

ABSTRACT Recent research on electronic records has produced proposals and models for adding functionality and procedural controls to information systems so that systems can protect the authenticity and integrity of records. This article reviews several electronic records management projects led by archivists and then explores recent developments in network security and authentication based on research outside the archival community. Focusing primarily on the development of "trusted systems" to support electronic commerce and digital publishing, the article evaluates alternative methodologies which offer partial solutions to electronic record-keeping concerns. It suggests ways in which methodologies for trusted systems are compatible with archival objectives, but also raises concerns about long-term preservation and accessibility.

Writers often use metaphors to connote complex concepts and little understood phenomena. Therefore, it is not surprising that metaphors permeate discussions of digital technologies and the fundamental changes they are spawning in commerce, education, communication, and social interaction. Metaphors such as the digital library, the electronic shopping mall, the gateway to experience and interaction, and cyberspace attempt to depict the essence of new technologically-enabled forms of interaction.[1] The record-keeping community has appropriated the metaphor of the wild frontier to describe the chaos of the

modern office as well as the boundless opportunities for specialists in record-keeping to establish a rule of law and tame the excesses of uncontrolled records creation, distribution, and storage.[2]

Recently, archivists have taken up the charge to tame the wild frontier through a variety of research and development projects which have proposed strategies for bringing order and integrity to the records of modern information systems. As records professionals, we have been breaking our own ground as we labour to solve record-keeping issues on the edge of the electronic frontier. Research on electronic record-keeping has reasserted the distinctions between records and other forms of information and reminded us that records are valued because they provide evidence of events, transactions, and decisions which can be used to verify or challenge what occurred immediately or long after the documented events transpired. Recent archival literature about electronic records begins with the assumption that information systems must have additional controls and functionality in order to establish and maintain the linkage between a record and its larger transactional context and to protect the authenticity and integrity of the record.

Identifying the unique attributes of record-keeping systems represents an important first step toward articulating the specific record-keeping and archival problems associated with computer-based information systems, but archivists should not assume that record-keeping professionals are the lone rangers on the wild frontier. This metaphorical space is becoming increasingly populated with other parties who are also trying to tame the wild frontier. In the areas of electronic commerce and digital publishing, which are discussed in detail later in this article, analogous concerns about the integrity and authenticity of electronic communications and digital documents are being addressed, and in some cases remedied, with policies, techniques, and standards that can be adapted to record-keeping requirements. It is important for archivists and records managers to understand parallel developments because some new strategies and methods may support record-keeping, while others may impede the achievement of archival objectives.

This article reviews recent research on electronic record-keeping within the archival community and then explores some recent developments in network security and authentication, focusing primarily on the development of "trusted systems" to support electronic commerce and digital publishing. I was motivated to write this article by the relatively narrow focus within the archival community on the research projects at the University of British Columbia and the University of Pittsburgh at the expense of several other significant projects, by what I perceive as a stalemate in the debates over the best way to address electronic record-keeping, and by a long-standing belief that archivists are reluctant to observe or accept external developments which have important implications for record-keeping systems. In doing so, I introduce research and development activities outside the record-keeping domain and suggest how

archivists and records managers might apply results from these activities to a more precise definition of record-keeping issues.

Recent Archival Research: Breaking Our Own Ground

The Pittsburgh and UBC Projects

For many archivists, electronic records research is synonymous with two large projects, "Functional Requirements for Evidence in Electronic Record-Keeping," conducted at the University of Pittsburgh from 1993 to 1996, and the University of British Columbia, Masters of Archival Studies project "The Preservation of the Integrity of Electronic Records," the first stage of which was completed in 1997.[3] It seems fitting to begin any discussion of electronic records research with these two projects, but in this article, the discussion will not end there. I will also examine several other archival research and development projects which have made significant contributions but have not shared in the limelight.

The Pittsburgh Project was an early response to a research agenda developed by the U.S. National Historical Publications and Records Commission (NHPRC) following an invitational conference held in January 1991.[4] The project represented a new point of departure for efforts within the archival community to address the problems of electronic records management and preservation. Unlike previous electronic records projects which were housed in archival institutions and designed to advance ongoing programmes, the Pittsburgh project moved electronic records research into an academic environment. The principal investigators, Richard Cox and James Williams, are faculty at the University of Pittsburgh who possess expertise in archival science and information technology. The project team included other faculty with backgrounds in computer science and information science, rounded out by the perspectives and expertise of David Bearman, the project's principal consultant. The project also supported several doctoral students in their studies of archival and information science.[5]

The project staff proposed to develop a set of "functional requirements" and to test the following six hypotheses about electronic record-keeping:

- First, there are basic organizational needs for creating and maintaining records which do not change when organizations keep records in electronic form. Electronic records systems, however, may be better equipped to satisfy some record-keeping needs which traditional systems did not handle well.
- Second, organizations can use policy, system design, standards, and implementation, or a combination of these tactics, to satisfy functional requirements for record-keeping.
- Third, record-keeping requirements vary among different types of business

applications, and organizations attribute varying degrees of risk to the failure to keep good records in different juridical, administrative, and operational environments.

- Fourth, software applications vary in their capacity to create and manage records, but software systems do not define organizational needs for keeping records.
- Fifth, all organizations in a similar business sector will have similar reasons and needs to create and keep records, but the organizations within a business sector will use different tactics and methods to meet those needs based primarily on their organizational culture.
- Sixth, after organizational culture, the next most important factor in determining whether an organization will maintain records adequately to meet its needs is the extent to which managers throughout the organization accept archival responsibility, followed by the technological capabilities of a designated archival or record-keeping programme.[6]

It is not surprising that the proposal responded directly to the research questions in the NHPRC research agenda, nor that it attempted to test through research some of the hypotheses proposed previously by Bearman.[7] Both Bearman and Cox were instrumental in shaping the NHPRC research agenda, Bearman as a member of the Planning Committee and Cox as the rapporteur and a contributor to the summary of the 1991 Working Meeting.[8]

The Pittsburgh Project produced four major products: 1) a list of conditions that organizations, information systems, and records must meet to ensure that evidence of business activities is produced when it is needed (the functional requirements); 2) a partial compilation of statutes, regulations, standards, professional guidelines, and other rules which specify when evidence of business activity is required, what form it should take, how long it should be kept, and other aspects of the format, content, maintenance, and accessibility of records (the warrant for record-keeping); 3) a formal definition of the conditions necessary to produce evidence expressed in a way that is unambiguous and consistent, and therefore can be used to develop software and test whether the necessary conditions have been met (the production rules); and 4) a set of data elements that uniquely identify each record, describe when, where, and by whom it was created, explain the physical and logical structure of the record, indicate terms and conditions for future access and use, and track subsequent uses of the record so that people and information systems in the future can ascertain the purpose, quality, and meaning of records (the metadata reference model). The Pittsburgh Functional Requirements and related products have been described and evaluated in countless articles and commentaries so I will not discuss the products in detail.[9] Rather, I will summarize the major contributions of the project and outline some of its shortcomings, particularly in light of the original goals and hypotheses.

The functional requirements provide an exhaustive inventory of conditions that organizations should consider to ensure that their policies, practices, systems, and records provide adequate and authentic documentation of their activities. The project staff used an inductive process to generate the functional requirements, which were based on earlier precedents, case studies, well known professional standards, and advice from experts.[10] Subsequent research on the formal warrant for record-keeping validated a need for all of the requirements, but also demonstrated that all of the requirements do not have equal weight and that in any specific record-keeping application many of the requirements are irrelevant, unnecessary, cost-prohibitive, or not justifiable on the basis of calculated risk analysis. In retrospect, the choice of the term "functional requirements" is unfortunate because the Pittsburgh model actually presents a higher level set of considerations from which more specific requirements can be derived for particular record-keeping applications.[11]

The concept of warrant and subsequent research on it by Wendy Duff is a significant contribution because it situates the mandates for creating and maintaining records in a legal, administrative, and professional context, and it presents a methodology for locating, compiling, and presenting the rules governing proper and adequate documentation in modern organizations.[12] The warrant, as it is expressed in legally binding regulations, organizational policy, or professional practice guidelines, provides archivists and records managers with a potentially powerful instrument for improving record-keeping that may prove more influential than arguments based on cost/benefit analysis or the needs of future researchers. In its current state of development, the record-keeping warrant assembled by the Pittsburgh project is in its formative stage of development with only a few hundred examples of specific regulations, guidelines, and professional best practices drawn almost exclusively from U.S. legislation, professional codes of practice, and international standards. Archivists and records managers could populate the warrant with additional examples or use the methodology to build locally relevant warrants for specific jurisdictions, types of business, professions, or institutions.

Several of the initial hypotheses proposed by the project team were not explored as fully as the functional requirements and warrant for record-keeping. The Pittsburgh research project detected variations in record-keeping requirements among different types of business applications and among organizations in different juridical, administrative, and operational environments, but the project staff were not able to specify how these factors affect record-keeping or influence the choice of strategies by organizations. Archivists and records managers will have to wait for more tests of the Pittsburgh model and more research on organizational and cultural variables before it will be possible to sort out which requirements are considered most critical in specific environments and which strategies and tools best support compliance in specific organizational settings.

In many respects, this is both the most interesting and the most disappointing aspect of the project. The project started with a simple hypothesis that there is a set of basic functional requirements for record-keeping and that these requirements can be satisfied through any or a combination of four tactics: policy, standards, systems design, and implementation. By the conclusion of the project, however, it was apparent that certain tactics are more effective for satisfying certain requirements and that comprehensive improvements in electronic record-keeping will require the right combination of policy, standards, system design methodologies, and implementation. Within this range of options, there is little research or evidence to provide guidance about which requirements are likely to carry the greatest weight in specific business domains or which tactics are most likely to succeed in organizations with different cultures and sensitivities to record-keeping issues. Nevertheless, the Pittsburgh project confirmed that satisfaction of record-keeping requirements depends on a combination of factors including the nature of the warrant, the position and mandate of the records management function, the nature and maturity of existing information systems, the perceived risk, the adoption of standards, and the availability of software to support electronic record-keeping. All of these factors must be considered against the backdrop of the even more elusive concept of organizational culture. Unfortunately, this aspect of the record-keeping problem got short shrift in the Pittsburgh project and it remains an area for considerable additional research.[13]

A major research project at the University of British Columbia, entitled "The Preservation of the Integrity of Electronic Records," was motivated by similar concerns about the difficulty of creating and maintaining records in electronic form. The project, under the direction of Luciana Duranti and Terry Eastwood at the School of Library, Archival, and Information Studies at UBC, set out to establish in principle what a record is and how it can be recognized in an electronic environment.[14] In addition to articulating the theoretical basis for identifying records, the project also proposed to determine which types of electronic systems generate records, to formulate criteria for segregating records, to define conceptual requirements for guaranteeing the reliability and authenticity of records, to articulate the administrative, procedural, and technical requirements, and to assess those methods against different administrative, juridical, cultural, and disciplinary perspectives.[15] The research, funded by the Social Sciences and Humanities Research Council of Canada (SSHRCC), commenced in April 1994 and the first phase of the project was completed in March 1997.[16]

The UBC project used a deductive method to "identify in a purely theoretical way both the byproducts of electronic information systems and the methods for protecting the integrity of those which constitute evidence of action."[17] The theoretical principles and concepts for the investigation were drawn from diplomatics and archival science. Like the Pittsburgh project, the findings and

products of the UBC project have been summarized in print and made available on the project web site.[18] The project staff developed a series of hypotheses regarding the creation of reliable records and the maintenance and preservation of authentic electronic records. The project staff theorize that the reliability and authenticity of electronic records are best ensured by embedding procedural rules in the overall records system and by integrating business and documentary procedures; that the reliability and authenticity of electronic records are best guaranteed by emphasizing their documentary context; and that the reliability and authenticity of electronic records can only be preserved if they are managed together with all the other records belonging to the same fonds. To achieve these objectives, the project staff posit that the life-cycle of the managerial activity directed to the preservation of the integrity of electronic records can be neatly divided into two phases: one phase directed to the control of the creation and maintenance of reliable and authentic active and semi-active records, and the other phase directed to the preservation of authentic inactive records. They also hypothesize that the integrity of electronic records is best preserved by entrusting the creating body with responsibility for their reliability and the preserving body with responsibility for their authenticity.[19]

The main contribution of the UBC project is a theory about the activities and entities involved in the genesis and preservation of records and a model that illustrates the relationships between entities and activities involved in managing archival fonds. Project staff have presented the initial results of the project as "conceptual findings," and it is important to recognize that these concepts are hypotheses that archivists and records managers will have to test in the real world before their validity can be determined. The statements presented as findings from the project would be described more accurately as assertions which require further refinement before generating hypotheses for testing. For example, finding 1.(ii) states that "the reliability and authenticity of electronic records are best guaranteed by instituting procedures that tighten and strengthen the archival bond, such as classification, registration, and profiling." This is a proposition that could be tested by comparing the proposed strategy with alternative methods for ensuring reliability and authenticity of electronic records. Recent innovations in authentication, system security, and trusted systems, which are described in detail in the next section of this article, offer alternatives which rely on encryption and digital signatures to authenticate transactions and prevent tampering.

The UBC researchers working with the U.S. Department of Defense (DoD) Records Management Task Force between January 1995 and October 1996 also developed models for aspects of record-keeping systems. Using a data and activity modeling technique based on IDEF (Integrated Definition Language), the project staff produced a business activity model and an entity model for "managing the archival fonds."[20] The activity model for Manage Archival Fonds consists of four subactivities: Manage Archival Framework, Create

Records, Handle Records, and Preserve Records, each of which has several subactivities. The subactivities for Handle Records, for example, include consign records to a central records system, retrieve records, copy records, annotate records, and remove records from a central records system.[21] The model is supported by a series of eight templates which define the necessary components of a record in a traditional and an electronic environment based on the principles of diplomatics and archival science, a glossary of 161 terms, and numerous procedural rules governing the activities involved in managing the archival fonds. Like the conceptual findings from the UBC project, the DoD model is an abstraction which represents "a model of functional requirements that are a model of an activity model of a theory of the application domain. The activity model for *Manage Archival Fonds* is a model of the theories of Archival Science and Diplomatics, and the other controls on this activity."[22] The templates, glossary of terms, activity and entity models, and rules provide a highly articulated theory of one possible approach to managing electronic records which should be tested along with alternative strategies.

Before turning to a discussion of projects that have tested and implemented portions of the recommendations from the Pittsburgh and UBC projects, it is important to consider the basis on which comparisons between the two projects might be made. The projects differ not only in the level of abstraction of their findings, but also in the scope of the terrain that they cover. The theoretical model proposed by the UBC project is intended as a generic model for managing archival fonds for all types of records in any juridical, administrative, or organizational context.[23] The Pittsburgh project also attempted to define a common set of functional requirements for evidence in record-keeping. Yet by recognizing the significance of the warrant, which is not a universal set of requirements but specific mandates and rules for record-keeping which vary in different national, business, and professional environments, the Pittsburgh project offers a methodology for designing record-keeping systems in specific environments rather than a model or template for all record-keeping and archival functions. Moreover, the Pittsburgh project assumed from the outset that the definition of record-keeping requirements could be separated from the means of satisfying the relevant requirements, thus leaving open the possibility of numerous options for implementation. In comparing the two projects it is important to consider how they differ in purpose, scope, and viewpoint. The purpose of such a comparison, however, is not to judge which approach is better, but to make educated choices about record-keeping and archival strategies that will succeed in achieving the goals of the organizations that need authentic and reliable records.

Pilot Projects and Implementations

Several projects have implemented aspects of the electronic record-keeping

models proposed by the Pittsburgh and UBC projects. Their experiences provide additional insights into the utility of the models and their relationship to larger organizational work processes. This section turns to four pilot implementations: Philadelphia's Electronic Records Project; the electronic records project at Indiana University; the Models for Action project at the New York State Center for Technology in Government; and the work of the DoD Records Management Task Force. After describing each effort briefly, I make some general observations and suggest areas for further research and development.[24]

The City of Philadelphia's Electronic Records Project was conducted in three phases from February 1995 through November 1997.[25] In addition to developing prototype policies and processes to improve electronic record-keeping generally in City government, the project focused on two transaction-based systems: a mid-sized human resources information system (HRIS) and an adjudication tracking system.[26] The main goal of the Philadelphia project was to evaluate the Pittsburgh functional requirements and develop methods to use contextual metadata to manage records in transactional systems. Project staff selected a core set of metadata elements from the larger set of elements enumerated by the Pittsburgh project. The requisite metadata, associated with each electronic record, makes the record "self-contained, self-sufficient, inviolable and hopefully acceptable as evidence for lawyers and judges, auditors, journalists and historians...."[27] Recommendations for incorporating record-keeping into a system redesign are embodied in the request for proposal for a new HRIS, and a test to retrofit record-keeping requirements is being conducted with the adjudication tracking system which is already in place. It remains to be seen whether vendors will be able to satisfy the record-keeping requirements in the RFP, how the record-keeping requirements will affect procurement costs, and how the City will respond if vendors either cannot meet the requirements or add significantly to the development costs in order to do so. This is an important test of new record-keeping models because, regardless of their value to archivists and records managers, they will have little impact if system developers cannot design systems that implement the models or if organizations are unwilling to pay to add record-keeping functionality to their information processing systems.

An electronic records project at Indiana University under the direction of Philip Bantin, University Archivist, and Gerald Bernbom, Associate Director and Senior IT Architect in the Office of Information Technologies, is using the Pittsburgh model to test how well existing information systems meet record-keeping requirements. Work on the project has focused on two large areas of university administration: Financial Management Services and Student Services.[28] The project team developed a methodology for defining the information categories necessary to generate evidence and for analyzing the extent to which existing information systems satisfy record-keeping requirements. Using functional decomposition of major business activities and conceptual data modeling,

the project team identified the actions, actors, business domain, and information generated for major business transactions. Turning to the Pittsburgh functional requirements as a guide, the project staff were then able to identify deficiencies in existing systems, but at this point in the project they have not yet developed definitive answers to the question of how best to address the problems they uncovered.

"Models for Action" is a joint project of the New York State Center for Technology in Government and the State Archives and Records Administration.[29] An underlying goal of the project is to translate the theoretical work on electronic records management into practical and implementable solutions. The project staff are using existing theory and methods for electronic record-keeping along with business process improvement/reeningeering methodologies to test the feasibility of incorporating record-keeping requirements into a new and improved system development methodology for state government. The project will produce a prototype system for issuing land use permits by the Adirondack Park Agency which will then be evaluated in terms of benefits to the agency, costs, and the extent to which the record-keeping functional requirements have been met. Project staff adapted the Pittsburgh functional requirements as well as requirements identified by the UBC project, the DoD Records Management Task Force, and the U.S. National Archives and Records Administration (NARA) to the specific concerns and processes of New York State government.[30] These requirements formed the basis for a Records Requirements Elicitation Component (RREC), which consists of a series of issues or questions about the business process, records, and system which analysts can use to identify record-keeping requirements in conjunction with business process analysis.[31] Work is underway to refine a broader Records Requirements Analysis and Implementation Tool which, used in conjunction with RREC, will help business process analysts and systems designers select appropriate methods for satisfying record-keeping requirements using management, policy, and technology strategies.

The work of the DoD Records Management Task Force drew heavily, but not exclusively, on the models proposed by the UBC researchers. For example, in developing functional baseline requirements for records management application software, the DoD Task Force members examined recommendations from both UBC and Pittsburgh and they incorporated many of NARA's regulations for electronic records management.[32] The major product of the DoD Records Management Task Force is a Design Criteria Standard for Records Management Application Functional Baseline Requirements.[33] The draft standard applies to all "records management applications (RMAs)," defined as "software used by an organization to manage its records."[34] The general requirements are quite straightforward, requiring that RMAs shall 1) manage organizational records regardless of storage media or other characteristics, 2) implement automated procedures to help capture records and

ensure their authenticity and reliability, 3) maintain electronic records in a manner that will prevent their alteration or premature destruction, and 4) accommodate information containing dates for the year 2000 and beyond, as well as dates from the current and previous centuries.[35] Although the DoD requirements do not prescribe methods for satisfying the requirements, they are oriented to applications which automate records management functions and provide an interface between the information processing environment and the records management system.

None of the projects discussed above has yet resulted in the implementation of a system which fully supports functional requirements for record-keeping, but the projects are far enough along to permit some general observations about electronic record-keeping systems and to suggest areas where further tests and additional research would be highly desirable. A common theme in all of the tests and pilot projects is pressure from the organizations developing systems and standards to simplify the models and limit the requirements to the minimum deemed absolutely necessary to satisfy organizational needs and requirements. The tendency toward simplification operates on several levels. Both the Models for Action Project and the DoD Records Management Task Force modified the functional requirements into a few general statements. The New York project defined three general requirements pertaining to 1) administering systems in accordance with best practices for information resource management, 2) creating or capturing records adequate to meet all business and record-keeping requirements, and 3) maintaining records so that they remain accessible and keep their integrity as long as needed. The latter two requirements are very similar to two of the four general DoD requirements which also include requirements to handle records in all media and to accommodate Year 2000 dates.[36]

The Indiana and Philadelphia projects applied the Pittsburgh functional requirements judiciously in keeping with known organizational risks and resource limitations. The Indiana researchers, after completing detailed analysis of a portion of the transactions associated with financial management and student services, concluded that "it might be necessary to limit the scope of our analysis to the primary and high priority functions and transactions as defined by a team of University personnel."[37] In Philadelphia, the Personnel Department identified twenty-eight "records-generating events" and used risk analysis to identify those transactions which were particularly prone to litigation or subject to audit.[38] Because HRIS will support a paperless human resources environment, the new system must ensure that electronic records are generated at each step in the workflow to meet audit and legal evidentiary requirements for litigation-sensitive activities. During the course of the analysis, the Electronic Records Group selected only five of the seven metadata layers proposed by the Pittsburgh project and grouped several of the discrete metadata elements into clusters of related elements. The project staff investigated alternatives for

capturing metadata as part of each application, outside the application, through the user interface, at the application programme interface (API), and as part of the system architecture, thus providing potential vendors with options for satisfying the metadata requirements with various system designs and architectures.[39] In one test of the core metadata, project staff found that all but four of the required metadata elements were generated automatically by the system. Careful selection of mandatory data elements combined with good systems design can limit the amount of data that users must supply in a record profile or as part of the records creation process.

Another striking similarity among the Indiana University, Philadelphia, and New York projects is their focus on business processes, systems, and transactions, and not on the records themselves. The Indiana project accepted the notion that a record is a consequence of a business transaction which has content, structure, and a business context. As Bantin and Bernbom argue, "[i]f we are refocusing our sights on the transaction producing the record rather than the record itself, it makes much more sense to focus records management not on the records but on managing the recordkeeping systems throughout their life cycle. If the systems which capture, maintain and support retrieval of records can be demonstrated to be sound, it is argued, the records within that system will be sound."[40] Models for Action has taken a similar tack by stressing Systems Reliability as one of the three categories of functional requirements. In that project, staff posit that the system should be administered in line with best practices in the information resource management (IRM) field to ensure the reliability of the records it produces.[41] Although this may appear to be a leap of faith or a displacement of responsibility to the system itself, new methods for security and authentication, discussed in the next section, offer reasons for increased confidence in the capabilities of systems to maintain reliable and authentic records.

Drawing general conclusions from the four pilot implementations discussed above is difficult because of wide variations in the organizational settings and the scope, purpose, and viewpoint of each of the projects. The DoD requirements come closest to a test of the UBC proposals because they encompass all records, regardless of storage media, and they propose an enterprise-wide solution for all DoD records primarily by automating procedures to help capture records and ensure their authenticity and reliability. The DoD standards apply to records management applications and they do not require reconsideration of work processes or redesign of existing systems. The Philadelphia project addressed some general elements of record-keeping through revised policies and project staff proposed an enterprise-wide metadata management system. Much of the research effort, however, focused on embedding record-keeping functions in a computer-supported business process and in applying data management methods, such as data mining, to extract metadata from an existing system. Rather than designing a record-keeping application which

could encompass paper and electronic records, the goal in this case was to ensure that the electronic records generated by new systems will be reliable and authentic as a means for eliminating paper records. The Indiana University project, in its functional analysis, and Models for Action, through its involvement with process analysis, delved more deeply into the relationships between the conduct of work and the generation of records, but neither project has yet reached a definitive conclusion about the feasibility of integrating record-keeping requirements into process redesign. Rather than presenting a consensus on electronic record-keeping strategies, these projects taken together suggest a variety of strategies that archivists and records managers could match with the goals, scope, and perspectives of the particular organizations where they have record-keeping oversight or responsibilities.

Meanwhile, Back at the Ranch...

Much of the archival research on electronic records is based on the assumption that electronic record-keeping systems are inherently inferior to traditional record-keeping systems in their capacity to create and maintain secure and authentic records. The ease of altering electronic records and the difficulty of proving their authenticity pose major impediments to trust in electronic record-keeping systems, not only for archivists and records managers, but also for the organizations and people who would like to rely on electronic systems for commerce and communication. While archivists have been breaking new ground and proposing ways to maintain reliable and authentic records, policy analysts, researchers, businesses, and software designers have been developing powerful new tools to ensure secure electronic transactions. Partial solutions to electronic record-keeping issues are emerging in a wide variety of application environments where concerns over the authenticity and reliability of digital documents create barriers to widespread deployment of electronic commerce, digital publishing, and secure global communications. Although these techniques may resolve some long-standing archival concerns about the authenticity of electronic records, research on electronic record-keeping generally has not incorporated potentially powerful methods developed outside the archival community.

Engagement of the information technology sector in archival research and development has been limited to sparse representation of faculty or research scientists on project staff or advisory committees, sporadic interactions with vendors and software developers, and occasional presentations by information technology experts at meetings and conferences. Archivists are not trained in research and development methodologies, lack experience with research, and typically do not follow the research underway in other fields which can be highly relevant to archival concerns.[42] The tendency to look inward for solutions to electronic record-keeping problems has several important implications

for record-keeping professionals. First, archivists and records managers may not recognize the potential of applying systems, methodologies, and techniques that address similar concerns for the authenticity, integrity, and preservation of records. Second, archival research projects may develop conceptual models and methodologies that are theoretically sound and robust according to archival principles, but that are technologically impossible or too expensive to implement. Third, because of the time lag in the research and development process, research based on assumptions about the capabilities of current technologies or the constraints of contemporary organizational policies and structures may well be obsolete by the time the research results are available for testing and implementation. Finally, archivists may miss opportunities to contribute to and influence major system redesign initiatives that organizations are planning or undertaking for other business reasons.[43] The following section of this article examines several initiatives under the general rubric of trusted systems as examples of the potential benefits that record-keeping professionals can reap from interdisciplinary perspectives on electronic record-keeping issues.

Trusted systems are defined as systems that can be relied on to follow certain rules at all times.[44] Record-keeping systems are a type of trusted system where rules govern which documents are eligible for inclusion in the record-keeping system, who may place records in the system and retrieve records from it, what may be done to and with a record, how long records remain in the system, and how records are removed from it.[45] Most record-keeping systems today are governed by procedural rules carried out by secretaries, file clerks, registrars, or records managers, or by the individuals who create and use records. Such systems can be trusted only to the extent that the personnel who carry out record-keeping procedures know and follow record-keeping rules at all times. Trust in record-keeping systems has eroded with the elimination of support staff in many organizations and the transfer of responsibility for creating and managing records from specialized personnel who handled classification, filing, retrieval, and disposition of paper records to administrators and professionals who generate and attempt to manage electronic records with personal computers and work stations. Common complaints about modern systems are that personnel involved in the creation and use of electronic records have too much authority and too much responsibility for record-keeping and that electronic systems circumvent the traditional procedural controls previously enforced by records management personnel.[46] With the increasing use of computer-based information systems, contemporary organizations are seeking ways to replace record-keeping systems which require that all participants in the record-generating process learn and follow the rules for record-keeping with systems where the rules are embedded in and enforced by software routines. In doing so, organizations are seeking trusted record-keeping systems that follow rules for records creation, maintenance, and preservation at all times.

The goal of developing trusted systems is embraced by a wide range of

interests from promoters of electronic commerce, to developers of digital libraries, to individuals seeking secure private communications. Trusted systems were developed initially to support Electronic Data Interchange (EDI) between trading partners who entered into agreements authorizing electronic computer-to-computer business transactions in conformance with mutually acceptable rules.[47] Early EDI systems relied on a combination of novel and well-established methods to build and maintain trust. The systems were novel because they permitted computer systems to execute transactions without human intervention for authorization or approval. Trust in the system was built on a combination of security procedures, prior established relationships among the trading partners, and formal, legally-binding agreements.[48] Early EDI systems relied for security on the use of proprietary systems with stringent access controls which were available only to designated trading partners, and electronic commerce still is most prevalent in applications involving a small number of trading partners with established, long-term relationships. The expansion of electronic commerce into personal and retail consumption depends, however, on the ability of individuals and organizations to communicate and conduct business using trusted systems that are not predicated on prior established relationships or formal contractual agreements.[49]

The development of trusted systems is also considered one of the fundamental underpinnings of the widespread growth of digital publishing and on-line exchange of intellectual property. In the case of digital publishing, owners of intellectual property want to control its reproduction, distribution, rendering, and extraction for reuse.[50] Digital publishers are developing trusted systems which limit the ways in which a consumer can use an intellectual work, collect and distribute payments to appropriate parties, and provide some degree of assurance to the consumer about the quality, accuracy, and authenticity of the work being distributed. Trusted systems for storage and distribution of digital intellectual property are especially relevant to archivists and records managers because they rely on the concept of a "trusted repository." The trust requirement for a digital repository is that the repository follows at all times and in all instances rules about how a digital work may be used.[51] Digital library applications enforce rules based primarily on copyright laws, but trusted repositories could be designed to enforce rules for record-keeping.

Parties to electronic commerce and promoters of digital publishing have defined a series of requirements, including authentication, confirmation, non-repudiation, assurance of payment, anonymity, integrity, recourse, and privacy, to address concerns about the authenticity and integrity of electronic transactions and the information that supports them. Authentication, confirmation, non-repudiation, and integrity are the most relevant of these requirements to electronic record-keeping issues. In electronic commerce, *authentication* refers to the process of verifying that the parties to an electronic transaction are who they purport to be. Authentication is necessary for both the buyer and

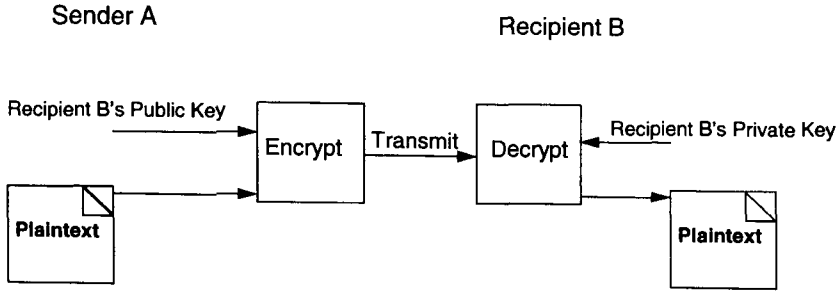

Figure One This process transmits a message that is secure because Recipient B needs his or her private key to decrypt the message.

seller, and it can also apply to the identification, nature, and quality of the goods and services that are being traded. Authentication techniques are also used to confirm that documents and e-mail messages originate from the person who claims to be the creator or sender and that the contents were not altered during or after transmission. *Confirmation* is the ability to prove that all of the parties to a transaction understand and agree to their roles and responsibilities in it. *Non-repudiation* refers to protections against an unjustifiable denial by any of the parties that the obligations to them were not fulfilled. Electronic transactions must also have *integrity* to protect the buyer from unauthorized payments for goods not purchased or for goods that are different from those presented by the seller.[52]

Trusted systems rely in part on technical solutions for the authentication and security of electronic communications. A general overview of these methods is important because they offer alternatives to the procedural controls with which archivists and records managers are most familiar.[53] By examining the methods available to satisfy requirements for trusted systems, the archival community could identify where the measures that organizations are taking to secure transactions for their own business needs are adequate, and where additional measures are needed to satisfy record-keeping requirements.

Public-key cryptography is one method used to validate that the person participating in a transaction is who he or she claims to be and that the communication itself is authentic. In principle, public key cryptography works with combinations of public and private keys. The sender of a message uses the recipient's public key, which is published or otherwise made available, to encrypt the message. The proper recipient is the only person with the private key needed to decrypt the message (see **Figure One**). This technique ensures that communications are secure, but not necessarily authentic. Because public keys are widely available, someone other than the real sender can use a public key that does not belong to them. Secure and authentic communications require the use of pairs of public and private keys by both parties (see **Figure Two**).

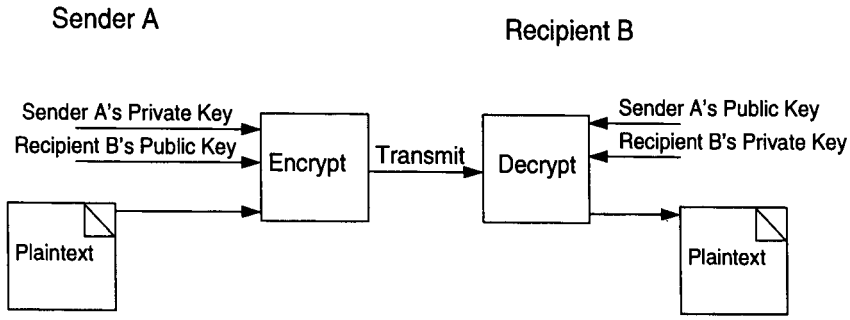

Figure Two This process transmits a message that is both secure and authentic. Recip-ient B needs his or her private key and Sender A's public key to decrypt the message. This proves that only Sender A could have sent the message to Recipient B.

Digital signatures and digital time/date stamps, appended to an electronic message or a digital document, add another level of security and validation. Using a combination of digital signatures, time/date stamps, and a technique called "hashing," it becomes possible to prove that a specific message was sent by a specific person at a certain point in time. A "hash value" is a very large number that is calculated using the entire document as input. If the recipient calculates the hash value of the document and it is identical to the hash value sent with the document in an encrypted form, he or she can be quite certain that the contents of the document have not been altered since it was signed and transmitted (see **Figure Three**). A combination of authentication, confirmation, non-repudiation, and integrity coupled with the techniques of digital signatures and time/date stamping offers a partial solution to concerns about the integrity and authenticity of electronic records. Widely available tools for authentication, confirmation, non-repudiation, and integrity could be incorporated into electronic record-keeping systems to ensure that trusted systems accept only authentic records, confirm that records creators understand and agree to the responsibilities associated with placing records in a trusted system, prohibit individuals from repudiating a record stored in a trusted system, and maintain the physical and intellectual integrity of the records.

The use of encryption to enhance security and authenticity of electronic communications is a good example of the complex interplay between technical solutions and issues of policy, standards, and implementation. This relatively simple technical solution has engendered extensive policy debates over privacy, the role and liability of trusted third parties, and the role of the state in protected communications. Encryption has stirred debates about appropriate technical standards, raised concerns about the potential impact of particular authentication methods on transaction processing efficiency, and fostered

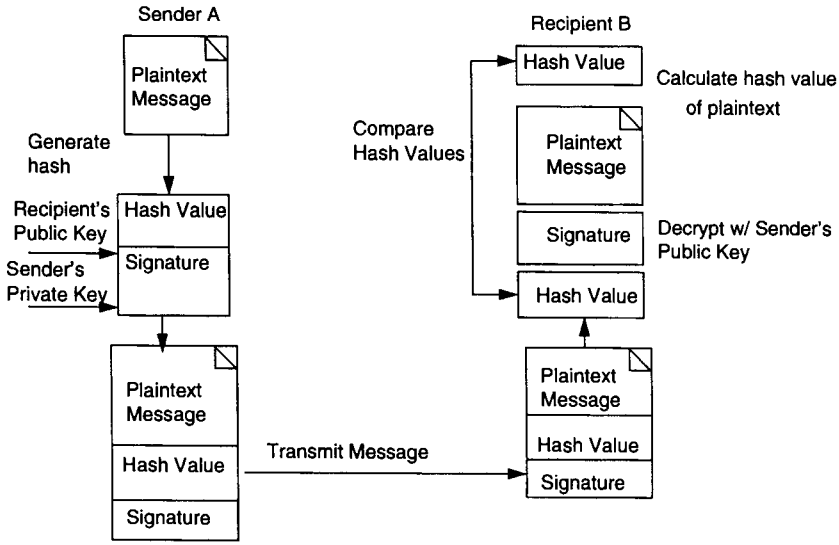

Figure Three If Recipient B can decrypt the signature with the sender's public key, he knows that only Sender A could have sent the message. If the hash values match, Recipient B knows that the contents of the message were not changed.

competition over who will develop and implement authentication processes and protocols.[54]

Organizational decisions and policies regarding whether and when to use encryption in the transmission and storage of digital information will have ramifications for future preservation and access. One policy area of particular relevance to archivists and records managers is key management or key recovery. There are numerous threats to security and authenticity in systems that use public key encryption because private keys can be lost, stolen, misused, or forgotten. To increase the reliability and security of systems based on public key cryptography, some organizations are engaging the services of trusted third parties that offer various types of authentication services. One popular approach is to use Certificate Authorities (CAs), which issue digital certificates that attest to the name, identity, and one or more attributes of the subscriber, and that contain the subscriber's public key and the CA's digital signature.[55]

Most organizations try to make authentication processes unobtrusive or invisible to the creators and recipients of electronic documents. One strategy is to bundle authentication processes with other system utilities and to integrate methods for authentication into e-mail utilities and web browsers.[56] Due to both the technical requirements for authentication and the added security gained by separating authentication from records creation, specialized busi-

nesses are offering various types of authentication services. Cybernotary services, for example, issue digital seals, time/date stamp certificates, and other authentication instruments for future verification that documents were created or filed at a specific date and time, and not changed subsequently. These services usually operate on a subscription or fee basis where a firm contracts with a trusted third party to provide authentication of documents and transactions.[57] While trusted third parties provide a vehicle for verifying the authenticity of digital documents, these services remain useful only as long as the trusted third party stays in business and continues to issue valid certificates.[58] Where trusted third parties are used, it is no longer adequate to think of the management of records as a simple relationship between records creators and records preservers as proposed by the UBC project.

Another controversial area is the provision for key recovery in cases where keys are lost, compromised, or stolen, or where a third party claims a right to access encrypted information. Law enforcement and national security agencies in the United States and elsewhere support centralized key recovery agents to permit wiretapping of otherwise unbreakable encrypted communications. Centralized key recovery agents, such as the Clipper Chip system proposed by the U.S. government, have been criticized on a number of grounds, including concerns over civil liberties if private keys were to be centralized, technical limitations, and unacceptable impediments to communications and business.[59] The authors of a recent report on risks associated with centralized key recovery systems questioned the business need for such a system, arguing that "key recovery, to the extent is has a private-sector application at all, is useful only for the keys used to protect irreproducible stored data."[60] For archivists and records managers, who are responsible for ensuring access to records with continuing value, the issue of key recovery and the management of private keys has tremendous significance. Businesses seem reluctant to leave key management exclusively in the hands of individual employees for fear of losing access to corporate records, while proposals for a central registry of keys under the control of a single government agency have been resisted successfully.

Storage of records in encrypted form is another area of concern because encryption adds additional levels of systems dependency on access to keys, proprietary encryption algorithms, hardware, and software. Most methods for encryption are secret and proprietary, and encryption can be hardware-based, software-based, or both. It is commonly assumed that some of today's encryption methods will be broken eventually by dedicated programmers with access to faster computers, and, to reduce this threat, cryptographers periodically introduce new encryption algorithms and increase the number of bits in hashes and digital signatures. Archivists and records managers who are in a position to influence record-keeping policies could discourage storage of records in encrypted form, while archivists who inherit encrypted records from records creators should anticipate significant technical impediments to future access to the records.

This discussion of some of the emerging technical solutions and associated policy issues is illustrative and not exhaustive. Similar arguments could be made about the insights that archivists and records managers can gain from research on emergent organizational forms and collaborative work which analyzes alternatives to rigid hierarchies and formal work processes. Likewise, new systems architectures which rely on agent-based systems rather than formal processes and procedures are introducing fundamental changes in the design, implementation, and capabilities of computer-based systems. Unless record-keeping models and records management strategies are sensitive to new approaches to work activities and the systems that support them, the solutions proposed by archivists will be anachronistic to the problems they are attempting to solve.

Forsaking the Silver Bullet

Recent research and development efforts within the archival community combined with new methodologies for trusted systems provide archivists with a variety of tools to enhance the integrity, reliability, and usefulness of electronic record-keeping systems. Nevertheless, archivists and records managers cannot ride into the sunset until we have clearer answers to a number of unresolved issues that will help organizations select the most appropriate strategies for electronic record-keeping from an increasing set of options. In a recent comparison of the findings of the UBC-MAS and Pittsburgh projects, Luciana Duranti and Heather MacNeil suggested that implementation of the Pittsburgh and UBC models in a variety of organizational settings would demonstrate which approach offers the most effective means of ensuring the integrity of electronic records.[61] Their proposal implies that archivists should choose a single approach from two possible options. The results of the research projects discussed here and the increasing availability of technical tools and services to support record-keeping challenge the assumption that there is a single best way to ensure the reliability, integrity, and preservation of electronic records. Rather than selecting a single model, archivists and records managers would be better served by identifying which combination of policies, standards, system design methodologies, and implementation tactics are most effective for the particular organizational, business, technological, and cultural environments that they are trying to influence.

Identifying effective record-keeping strategies requires not only sensitivity to relationships between organizations and their record-keeping systems, but also greater clarity about organizational goals and objectives in addressing record-keeping issues. The choice of strategies will vary depending on whether organizations are seeking solutions that encompass existing record-keeping systems or only new systems as they are designed; whether the objective is to include hybrid systems with paper and electronic records, or only electronic records; whether an organization is seeking an enterprise-wide solution for all

of its records, or intends to use specific methodologies tailored to the requirements and technology of each system; and the extent to which the analysis and redesign of work processes is integrated with the design of record-keeping systems. If archivists blur these distinctions or confuse these goals, they may recommend solutions that are impractical or even inappropriate for the specific record-keeping problem at hand.

From an archival perspective, records should be controlled transparently without regard to their physical format or characteristics. Yet imposing this rigid requirement on all record-keeping systems may limit the options available to organizations that are seeking a sharp break from past practices as they attempt to adopt paperless systems or as they replace an older generation of technology which supported hybrid paper and electronic systems with electronic record-keeping systems. For example, record-keeping projects which have to incorporate legacy systems – whether paper or electronic – will not be able to utilize many of the advanced security and authentication processes discussed in this article. Hybrid systems are more difficult to fit into emerging models for trusted systems because traditional paper-based records are generated outside of the boundaries of the electronic system and they only become subject to its automated controls by incorporating them into the system through digitization or by building control mechanisms such as document profiles for paper and electronic records. Organizations that are developing paperless transaction systems have more latitude to design novel solutions to the problems of authenticity and integrity because they can rely on tools such as encryption and automatic capture of metadata which are not possible with paper records.

Organizations that are seeking enterprise-wide solutions based on organizational policy, enforcement of procedures, and choice of system architectures may approach electronic record-keeping differently from organizations that require solutions and strategies for specific business processes or functions. This is one of the principal differences between the approaches taken by the UBC and Pittsburgh projects. The UBC project aimed toward defining a set of principles and procedures that an agency could apply to manage its records regardless of the format of the records or the systems used to generate them. While the Pittsburgh project also defined general requirements for evidence in record-keeping, the model is more amenable to the design of specific business applications which incorporate records capture, description, segregation, and preservation as an integral part of the normal business process.

The pilot implementations in Philadelphia, New York State, and at Indiana University have emphasized particular business processes or applications. Research on the warrant for record-keeping further supports the hypothesis that record-keeping requirements are specific to particular business domains. But there are also countervailing pressures which encourage enterprise-wide solutions to electronic record-keeping. Pilot implementations of all of the electronic

record-keeping models illustrate the time consuming and labour intensive nature of developing detailed functional analysis for each application, identifying specific record-keeping requirements, and integrating these requirements into new system designs. These experiences raise doubts about the feasibility of extending such a detailed analysis to all business processes and all of the records of a complex modern organization.

Archivists and records managers will have to face the question of how tightly record-keeping can be integrated into normal business processes and where to draw the line between the way organizations do their work and the way they keep their records. There is a common theme in the recent research that it is highly desirable to incorporate record-keeping into normal business processes in order to strengthen the link between records and their transactional context, limit the amount of discretion that people have about when to create or capture records, decrease the time and effort that people have to invest in managing records, and reduce opportunities for human error. Achieving the goal of record-keeping processes that are completely transparent to the records creator, however, will require engagement by archivists in business process redesign and wide scale adoption of tools, such as the Records Requirements Elicitation tool developed by the Models for Action project, as an integral part of business process and business system design.

The Models for Action project is most explicit in its goals to find ways to incorporate consideration of record-keeping into business process analysis and redesign and to include provisions for record-keeping in the design of new systems. One assumption underlying Models for Action was that organizations have come to view records management as an additional layer of activity that does not contribute to the achievement of organization-specific business objectives.[62] In developing practical tools, the Models for Action project staff shifted their focus from system design methodologies to business process analysis in an effort to make satisfying records management and archival requirements part of the business process and not an independent, additional activity.[63] Staff of the Indiana University project are not yet certain whether to maintain records within existing information systems or to create a separate record-keeping system apart from each active information processing system, although their preference is to incorporate record-keeping functions into information systems.[64] The Philadelphia project, with its focus on detailed analysis and prototyping of a few small and mid-sized applications has "side-stepped" the question of whether "adding the recordkeeping functionality to each system individually is better than an enterprise-wide solution, such as an integrated paper and electronic system."[65] Of the projects discussed here, only the DoD standard for Records Management Applications proposes an enterprise-wide solution using separate records management applications that can handle paper and electronic records with an interface between the records creation processes and the records management system.

Evidence from this review of emerging methods for secure and authentic electronic communications shows that the division of responsibility, accountability, and jurisdiction over record-keeping is becoming more complex than a clear line between the records creator and the records preserver. Increasingly, verification of the authenticity of records and other forms of communications is handled by technical means through a combination of encryption, digital signatures, and time/data stamping techniques which, if properly employed, make forgery, alteration, or unauthorized deletion virtually impossible. Trusted third parties, which have no interest in tampering with the records, are an increasingly important element in record-keeping processes. Recent research also illustrates that strategies and tactics for electronic record-keeping rarely involve a simple choice between policy, standards, systems design, and implementation. Rather, archivists and records managers need to pursue the right combinations of policies, standards, and system design methodologies that organizations can implement and that offer solutions which are affordable and commensurate with the risks and benefits involved. More importantly, archivists and records managers may be the only discipline that can bring the long-term perspective to the process of developing policies, adopting standards, and developing systems in a way that enables future use and reuse of electronic records.

The wild frontier is becoming more civilized and it is also becoming more complex. Rather than seeking the silver bullet – whether it is the sheriff with a record-keeping warrant, the notary with his digital seals, or the judge to enforce the rule of archival law – the record-keeping community needs to refine its solutions so that they meet varied organizational needs and operate compatibly with increasingly complex systems and organizations. Like the taming of the real frontier, record-keeping professionals no longer need to make all of their own tools or grow all their own food. The frontier of cyberspace, while still evolving, now offers some tools and services which can be adapted and used to support electronic record-keeping. It is incumbent upon record-keeping professionals, however, to help organizations select appropriate tools, consider the long-term implications of their use, continue research and development, and implement and evaluate the various approaches to electronic record-keeping – not with an eye toward selecting the one best method – but to learn which strategies for electronic record-keeping mesh with specific organizational goals and broader social needs for reliable and authentic records.

Notes

* The author thanks Richard Barry, John McDonald, and Lisa Weber for their extensive and valuable comments on an earlier version of this article.

1 For an extended discussion of metaphors for the Internet, see Mark Stefik, ed., *Internet Dreams* (Cambridge, Mass., 1996).

2 John McDonald, "Managing Records in the Modern Office: Taming the Wild Frontier," *Archivaria* 39 (Spring 1995), pp. 70–79.

3 University of Pittsburgh, School of Library and Information Science, "Functional Requirements for Evidence in Electronic Recordkeeping," James Williams and Richard J. Cox, principal investigators, NHPRC Grant #93–003; and University of British Columbia, School of Library, Archival, and Information Studies, "The Preservation of the Integrity of Electronic Records," Luciana Duranti, principal investigator, Terry Eastwood, co-investigator, and Heather MacNeil, research assistant, funded by the Social Sciences and Humanities Research Council of Canada.

4 U.S. National Historical Publications and Records Commission, *Research Issues in Electronic Records, Report of the Working Meeting* (St. Paul, Minn., 1991).

5 Two of the doctoral students supported by the project, Wendy Duff and David Wallace, have completed doctoral work on electronic record-keeping issues. See Wendy Duff, "The Influence of Warrant on the Acceptance and Credibility of the Functional Requirements for Recordkeeping," (Ph.D. Dissertation, University of Pittsburgh, School of Information Sciences, 1996); and David Wallace, "The Public's Use of Federal Recordkeeping Statutes to Shape Federal Information Policy: A Study of the PROFs Case," (Ph.D. Dissertation, University of Pittsburgh, School of Information Sciences, 1997).

6 University of Pittsburgh, School of Information and Library Studies, grant proposal for "Variables in the Satisfaction of Recordkeeping Requirements for Electronic Records Management," (August 1993, rev. July 1994), <www.lis.pitt.edu/~nhprc/IProposal.html>, as last modified: 9/18/96.

7 The idea that policy, standards, systems design, and implementation represented alternative tactics for satisfying record-keeping requirements was first expressed by David Bearman in "Diplomatics, Weberian Bureaucracy, and the Management of Electronic Records in Europe and America," *American Archivist* 55 (Winter 1992), pp. 168–80. This article stressed the influence of organizational culture and national traditions on the choice of tactics.

8 The other members of the Planning Committee were Lila Goff, Assistant Director of the Minnesota Historical Society (which sponsored the Working Meeting), chair; John McDonald, National Archives of Canada; Lisa Weber, then program director for electronic records at the NHPRC; and this author.

9 Readers who are unfamiliar with the Pittsburgh Project will find detailed reporting on its purpose, hypotheses, methodology, and results on the project web page at <www.lis.pitt.edu/~nhprc/>. For published summaries about the project, see Kimberly J. Barata, "Functional Requirements for Evidence in Recordkeeping: Further Developments at the University of Pittsburgh," *Bulletin of the American Society for Information Science* 23, no. 5 (June/July 1997), pp. 14–16; David Bearman, "Archival Data Management to Achieve Organizational Accountability for Electronic Records," *Archives and Manuscripts* 21, no. 1 (1993), pp. 14–28; David Bearman, "Record-Keeping Systems," *Archivaria* 36 (Autumn 1993), pp. 16–36; Richard J. Cox, "The Record: Is It Evolving?" *Records & Retrieval Report* 10 (March 1994), pp. 1–16; Richard J. Cox, "The Record in the Information Age: A Progress Report on Research," *Records & Retrieval Report* 12, no. 1 (January 1996), pp. 1–16; Richard J. Cox, "Re-Discovering the Archival Mission: The Recordkeeping Functional Requirements Project at the University of Pittsburgh, A Progress Report," *Archives and Museum Informatics* 8, no. 4 (1994), pp. 279–300; and Wendy Duff, "Ensuring the Preservation of Reliable Evidence: A Research Project funded by the NHPRC," *Archivaria* 42 (Fall 1996), pp. 28–45.

10 This author was one of the participants in the First Experts Meeting held in Pittsburgh in May 1993, which included experts with professional training and experience in the areas of archives, electronic records management, information system design, and auditing. This meeting was the culmination of the first stage of an iterative process through which the functional requirements were further refined over the course of the next two years. This author also participated in the Second Experts Meeting held in February 1996.

11 Use of the term "functional requirements" has caused confusion among archivists who are unfamiliar with this concept and among some systems analysis who use the term in a more specific way. In commentaries on the project at the 1995 SAA meeting in Washington, D.C.,

P.C. Hariharan, a computer scientist, and Seamus Ross, a specialist in humanities computing, both commented on difficulties with the terminology chosen by the project. Luciana Duranti and Heather MacNeil also contend that the Pittsburgh project's use of functional requirements is not the common usage in computer science (Luciana Duranti and Heather MacNeil, "The Protection of the Integrity of Electronic Records: An Overview of the UBC-MAS Research Project," *Archivaria* 42 (Fall 1996), p. 63. While I agree with many of these points, I do not believe that the project's use of the term functional requirements invalidates its findings or contributions. Substituting a term like "principles," "desirable attributes," or even "objectives for evidence" in record-keeping would provide a more descriptive designation for what are called functional requirements.

12 Duff, "The Influence of Warrant on the Acceptance and Credibility of the Functional Requirements for Recordkeeping;" and "Increasing the Acceptance of Functional Requirements for Evidence," *Archives and Museum Informatics,* 10, no. 4 (1996), pp. 326–51.

13 The fact that the Pittsburgh project was unable to investigate all of its initial hypotheses is not intended as a criticism of the project. All too often, researchers are unable to investigate all aspects of a research problem because of methodological, logistical, and time constraints. The project did produce three very valuable reports on its preliminary forays into organizational culture. See David Wallace, "Satisfying Recordkeeping Functional Requirements: The Organizational Culture Variable," February 1994; Wendy Duff and David Wallace, "Organizational Culture;" and David Thomas "Business Functions: Toward a Methodology," February 1994, unpublished papers available from <http://www.lis.pitt.edu/~nhprc/IContents.html>. Reporting on the difficulties that the project faced in investigating the "organizational culture variable" would be beneficial to other researchers who might embark on similar studies.

14 Luciana Duranti and Terry Eastwood, "Protecting Electronic Evidence: A Progress Report on a Research Study and its Methodology," *Archivi & Computer* V, no. 3 (1995), pp. 214–15.

15 Duranti and Eastwood, "Protecting Electronic Evidence," p. 215.

16 During the initial stages of this project, this author participated in the project's site visits to the national archives of Sweden and the Netherlands and to several government agencies in both countries in April and May 1995.

17 Duranti and Eastwood, "Protecting Electronic Evidence," p. 214.

18 Duranti and Eastwood, "Protecting Electronic Evidence," (1995), pp. 213–50; Luciana Duranti, Heather MacNeil, and William E. Underwood, "Protecting Electronic Evidence: A Second Progress Report on a Research Study and its Methodology," *Archivi & Computer* VI, no. 1 (1996), pp. 37–69; Heather MacNeil, "Protecting Electronic Evidence: A Final Progress Report on a Research Study and Its Methodology," *Archivi & Computer* VII, no. 1 (1997), forthcoming; and Duranti and MacNeil, "The Protection of the Integrity of Electronic Records: An Overview of the UBC-MAS Research Project," *Archivaria* 42 (Fall 1996), pp. 46–67. The current address of the project web site is: <www.slais.ubc.ca/users/duranti/>.

19 Duranti and MacNeil, "The Protection of the Integrity of Electronic Records," pp. 58–62.

20 The U.S. Department of Defense (US DoD) Records Management Program Management Office and the University of British Columbia (UBC) Master of Archival Studies Research Team, "Genesis and Preservation of an Agency's Archival Fonds," <www.slais.ubc.ca/users/duranti/>; and W. Underwood, L. Duranti, D. Prescott, and Col. M. Kindl, "Extensions of IDEF Methodology Based on US Department of Defense Experience in Reengineering Records Management," World Multiconference on Systemics, Cybernetics and Informatics, Sci '97, Focus Symposium on Business Process Reengineering, Caracas, Venezuela, 7–11 July 1997, pre-print, n.p.

21 Duranti, MacNeil, and Underwood, "Protecting Electronic Evidence," pp. 47–52. A current version of the activity and entity models is available on the project web site <www.slais.ubc.ca/users/duranti/>.

22 Underwood, et al., "Extensions of IDEF Methodology Based on US Department of Defense Experience in Reengineering Records Management," n.p.

23 Duranti and MacNeil, "The Protection of the Integrity of Electronic Records," pp. 62–63.

24 Other noteworthy projects that have also tested electronic record-keeping requirements include projects at the World Bank, Astra AB, and several other pharmaceutical companies. See Clive Smith, "Implementation of Imaging Technology for Recordkeeping at the World Bank," *Bulletin of the American Society for Information Science* 23, no. 5 (June/July 1997), pp. 25–29; Ulf Anderson, "Short version of the Seasam Report. Philosophy and rules concerning electronic archives and authenticity," *Proceedings of the DLM-Forum on electronic records, Brussels, 18–20 December 1996*, (Luxembourg: Office of Official Publications of the European Commission, 1997), pp. 175–89; and Philip Lord, "Strategies and tactics for managing electronic records; a view from the pharmaceutical industry," *Proceedings of the DLM-Forum*, pp. 168–74.

25 This project, directed by David Weinnerg, Deputy Commissioner of the Records Department and staffed by Mark Giguere, Electronic Records Manager, was funded in part by three grants from the National Historical Publications and Records Commission (95–031, 96–089, and 97–001). This author was a consultant to the project in 1995 and 1996.

26 Mark D. Giguere, "Automating Electronic Records Management in a Transactional Environment: The Philadelphia Story," *Bulletin of the American Society for Information Science* 23, no. 5 (June/July 1997), p. 19.

27 Giguere, "Automating Electronic Records Management," p. 18.

28 Philip C. Bantin and Gerald Bernbom, "The Indiana University Electronic Records Project: Analyzing Functions, Identifying Transactions, and Evaluating Recordkeeping Systems. A Report on Methodology," *Archives and Museum Informatics*, 10, no. 3 (1996), pp. 246–66.

29 Models for Action is housed at the CTG and funded by a grant from the NHPRC (96–023). Principal staff are Kristine Kelly, Research Associate at CTG, and Alan Kowlowitz, SARA.

30 New York Center for Technology in Government, Models for Action, "Draft Functional Requirements to Ensure the Creation, Maintenance, and Preservation of Electronic Records," Center for Technology in Government, 1997 <www.ctg.albany.edu/projects/er/freqv2..tm1>.

31 Models for Action: Developing Practical Approaches to Electronic Records Management and Preservation, Report to NHPRC for the time period from 10/1/96 to 3/29/97, Center for Technology in Government, 1997 <www.ctg.albany.edu/projects/er/secondrpt.html>.

32 U.S. Department of Defense, Records Management Task Force, "Electronic Records Management Test Requirements: Academic and Industry Review," 16 May 1995, <http://www.dric.dla.mil/c3i/recmgmt.html>.

33 U.S. Department of Defense, "Department of Defense Design Criteria Standard for Records Management Application Functional Baseline Requirements," (DoD STD-5015.2), 8 April 1997.

34 U.S. Department of Defense, "Design Criteria Standard for Records Management Application Functional Baseline Requirements," p. 14.

35 U.S. Department of Defense, "Design Criteria Standard for Records Management Application Functional Baseline Requirements," p. 14.

36 Alan Kowlowitz and Kristine Kelly, Models for Action: Developing Practical Approaches to Electronic Records Management and Preservation," *Bulletin of the American Society for Information Science* 23, no. 5 (June/July 1997), p. 22.

37 Bantin and Bernbom, "The Indiana University Electronic Records Project," p. 264.

38 Philadelphia Electronic Records Project, "RFP Text," portions of the RFP for the HRIS that refer to electronic record-keeping, issued 15 March 1996 <www.phila.gov/city/departments/ermskfp3.html>.

39 It is important to note that there are at least four different methods for structuring and managing metadata: 1) embedding the metadata in the record itself; 2) encapsulating each record with a set of metadata elements (also called wrapping); 3) associating records with a separate file of metadata; and 4) linking records and metadata with explicit common fields or live links. The preferred approach to metadata management has important implications for system architec-

ture and design. The most critical issue for record-keeping professionals, however, is defining the required metadata and understanding the implications of various options for implementation. The approach to metadata management may have significant implications for whether electronic records are managed on the item-level or in larger aggregations.

40 Bantin and Bernbom, "The Indiana University Electronic Records Project," p. 250.

41 Kowlowitz and Kelly, "Models for Action," p. 22.

42 One of the major conclusions of the 1996 Conference on Electronic Records Research and Development was that more differentiation is needed in archival research between basic research and development, which is best carried out in universities and research laboratories, and pilot testing, implementation, and evaluation, which are best done in organizations with ongoing responsibilities for records generation, maintenance, and preservation. See *Electronic Records Research and Development*, Report of an Invitational Conference held at the University of Michigan, 28 and 29 June 1996, sponsored by the Bentley Historical Library and the School of Information, Ann Arbor, 1997; <www.si.umich.edu/e-recs/>. The need to engage other disciplines in archival research is not limited to expertise in software development and systems design. Cognitive psychology, organizational theory, management, and information policy are some of the related fields which also produce research results that are highly relevant to archival issues.

43 A good example of a missed opportunity is the attention focused on and the investments in the Year 2000 problem. Businesses and government agencies are investing billions of dollars to redesign systems or implement workarounds for legacy systems with truncated dating systems. To my knowledge, archivists have made no attempts to integrate system redesign efforts to enhance the record-keeping capabilities of systems with the considerable investments being made to resolve Y2K problems.

44 Mark Stefik, "Letting Loose the Light," in *Internet Dreams*, p. 226.

45 This is a high-level abstraction of the rules governing record-keeping systems. In different juridical, temporal, cultural, and business contexts, the criteria for complying with these rules vary widely. Some record-keeping systems are governed by very general principles while others have elaborate rules and strict controls. The critical issue for trusted systems is not that rules must be extensive and elaborate but that they are known and followed at all times.

46 John McDonald, "Taming the Wild Frontier," pp. 71–72. This issue was also raised by judges in the series of cases against the U.S. government involving use of the PROFs e-mail system by personnel in the Executive Office of the President. In his 6 January 1995 ruling, Judge Richey declared that "The court also finds that the Defendants [sic] record keeping procedures are arbitrary and capricious because there is no oversight of the agency staff by the record keeping personnel. The agency staff make the decision in every instance whether computer material is a federal record that must be saved." Opinion of Judge Charles Richey in Armstrong v. Executive Office of the President, U.S. District Court for the District of Columbia, 6 January 1993, C.A. No.89–0142 CRR. In a recent ruling on NARA's General Records Schedule 20, Judge Paul L. Friedman also found that the general records schedule for electronic records gave agency personnel too much discretion in determining what is and is not a record. See Opinion of Judge Paul L. Friedman in Public Citizen, et al v. Carlin, U.S. District Court for the District of Columbia, 22 October 1997, No. 96–2840 (PLF).

47 For an example of the types of rules recommended for EDI transactions, see Electronic Messaging Services Task Force, American Bar Association, "The Commercial Use of Electronic Data Interchange: A Report and Model Trading Partner Agreement," *The Business Lawyer* 45 (June 1990), pp. 1645–1747.

48 Scott Hamilton, "E-Commerce for the 21st Century," *Computer* 30, no. 5 (May 1997), p. 44–46.

49 One survey, conducted in January 1997, estimated that 50 million people over the age of sixteen in the United States and Canada had Internet access, and about 37 million had access to the world wide web. See Ajit Kambil, "Doing Business in the Wired World," *Computer* 30, no. 5 (May 1997), p. 56. Another study estimated that half of Internet users in the U.S. purchased

goods on-line in 1996, but this translates into a mere 5.4 per cent of the U.S. population. See Hamilton, "E-Commerce for the 21st Century," pp. 44–45.

50 Mark Stefik, "Trusted Systems," *Scientific American* 276 (March 1997), pp. 78–81.

51 Stefik, "Letting Loose the Light," pp. 238–41.

52 A. Michael Froomkin, "The Essential Role of Trusted Third Parites in Electronic Commerce," *Oregon Law Review* 49 (1996), non-paginated electronic version available at <www.law.miami.edu/~froomkin/articles/trusted1.htm>.

53 A detailed technical description of security issues and measures is beyond the scope of this article. For a comprehensive overview written for a lay audience, see Bruce Schneier, *E-Mail Security: How to Keep Your Electronic Message Private* (New York, 1995).

54 A recent article in the *New York Times* reported on a backlash against a security system for electronic commerce called SET (Secure Electronic Transactions), which is being introduced by the credit card industry, because it is too slow, too expensive, and cumbersome for users. See Saul Hansel "New Security System for Internet Purchases Has Its Doubters," *The New York Times* National Edition, (24 November 1997), C1, C6.

55 Froomkin, "The Essential Role of Trusted Third Parties in Electronic Commerce," n.p. Because CAs are a recent development, several methods have been proposed to increase their trustworthiness. Government entities could license CAs and permit firms that meet standards set by the regulating body to issue certificates; one or more government agencies could act as CAs; or market forces could regulate the quality of CAs on the assumption that firms which do not provide accurate and reliable certificates will be driven out of business.

56 Hamilton, "E-Commerce for the 21st Century," p. 46.

57 Charles R. Merrill, Esq., "The Digital Notary™ Record Authentication System – A Practical Guide for Legal Counsel on Mitigation of Risk From Electronic Records," 22 June 1995, available from Surety Technologies, Inc., <www.surety.com>.

58 Froomkin, "The Essential Role of Trusted Third Parties in Electronic Commerce," n.p.

59 Hal Abelson et al., "The Risks of Key Recovery, Key Escrow and Trusted Third-Party Encryption," 27 May 1997. The latest version of this document can be found on the world wide web at <http://www.crypto.com/key_study>.

60 Abelson et al., p. 5.

61 Duranti and MacNeil, "The Protection of the Integrity of Electronic Records," p. 63.

62 This assumption was based in part on research conducted at the New York State Archives and Records Administration for the Building Partnerships Project. See New York State Education Department, State Archives and Records Administration, *Building Partnerships: Final Report and Working Papers*, Albany, NY, available on the world wide web at: <http://unix6.nysed.gov/pubs/build.htm>.

63 Models for Action: Developing Practical Approaches to Electronic Records Management and Preservation, Report to NHPRC for the time period from 10/1/96 to 3/29/97, p. 1.

64 Bantin and Bernbom, "The Indiana University Electronic Records Project," pp. 264–65.

65 Giguere, "Automating Electronic Records Management," p. 17.