Educating for trust

Article *in* Archival Science · November 2011

DOI: 10.1007/s10502-011-9152-3

2 authors:

Luciana Duranti
University of British Columbia - Vancouver
69 PUBLICATIONS **705** CITATIONS
SEE PROFILE

Corinne Rogers
University of British Columbia - Vancouver
20 PUBLICATIONS **47** CITATIONS
SEE PROFILE

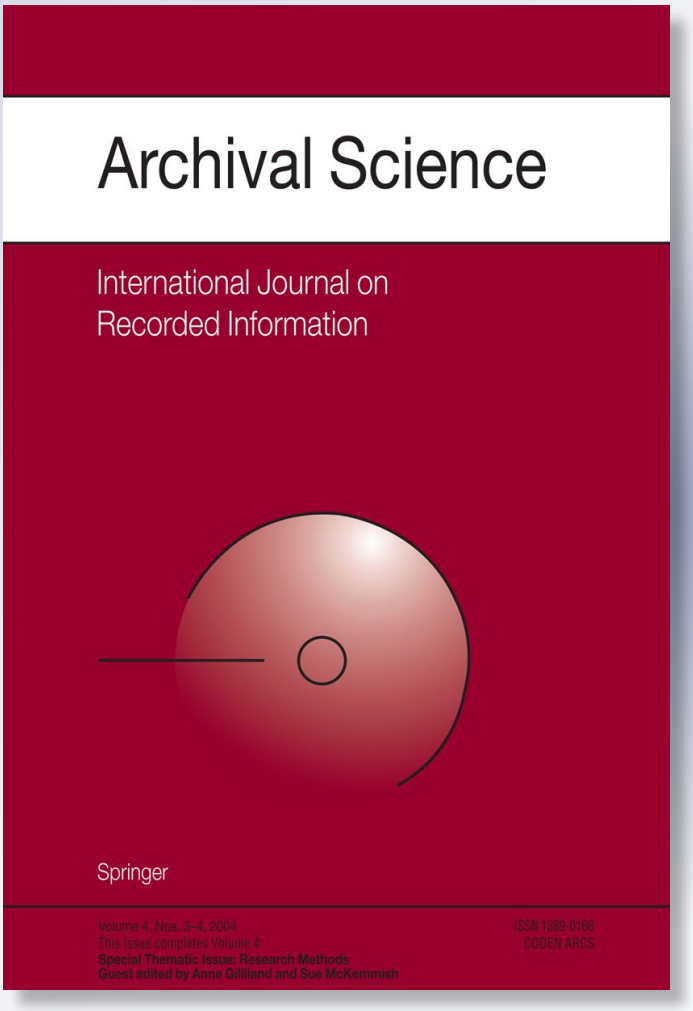
Educating for trust

Luciana Duranti & Corinne Rogers

Archival Science
International Journal on Recorded Information

ISSN 1389-0166
Volume 11
Combined 3-4

Arch Sci (2011) 11:373-390
DOI 10.1007/s10502-011-9152-3



Springer

Arch Sci (2011) 11:373–390
DOI 10.1007/s10502-011-9152-3

ORIGINAL PAPER

Educating for trust

Luciana Duranti · Corinne Rogers

Published online: 24 September 2011

Abstract Rapid technological advances are fuelling trust requirements and concerns about public and private sector records alike. To guarantee the reliability and authenticity of records requires a framework of policies, procedures, technologies, and intentional action or intervention by "trusted custodians" who have the knowledge required for attesting to and ensuring the continuing authenticity of the records. Records professionals have claimed the role of trusted keepers of the authentic record of our times, but how do they earn that trust? To begin, by acquiring competence. In order to define what kind of education would contribute to qualifying records professionals as competent, it is necessary to identify the components of knowledge they require and the role that society at large expects of them. The responsibilities and challenges presented by managing digital records through time are ones that records professionals should not meet in isolation. In order for records to be able to serve as evidence of actions and events, they must be protected as such. Records-related knowledge requirements are being articulated in the related disciplines of archival science and records management, law, digital forensics, and information assurance and cyber-security. The need for interdisciplinary knowledge to understand and manage the complexities of digital records is being realized in new research alliances that foster the development of knowledge that can support the role of trusted keepers of the authentic record of our times. One such alliance is the Digital Records Forensics Project at the University of British Columbia.

Keywords Trust · Trusted recordkeeper · Digital forensics · Authenticity · Trustworthiness

L. Duranti · C. Rogers (✉)
School of Library, Archives and Information Studies, University of British Columbia, Vancouver, BC, Canada
e-mail: corinne.rogers@gmail.com

L. Duranti
e-mail: luciana@mail.ubc.ca

Introduction

How can we know when digital records are trustworthy? That they are what they purport to be, that they are reliable and their contents accurate? What assurances do we have that our personal information, our identity and intellectual property are safe and secure when we engage in Internet transactions and activities, whether we are making a purchase from iTunes or Amazon, updating Facebook or Twitter, blogging, or filing our taxes, to name but a few possibilities? We must trust the computer technologists who configure, monitor and protect network systems, and the records professionals responsible for records to be created, maintained and used according to policies and procedures that protect them from alteration, falsification or degradation. We must trust the digital archivists and curators who have claimed for themselves the role of trusted keepers of the authentic record of our times. To earn our trust, recordkeepers must demonstrate that they have no reason to alter the records and no interest in allowing others to do so, and must have the knowledge necessary to implement procedures that ensure the continuing identity, integrity and accuracy of the records.

The level of trust required is proportional to the sensitivity of the material to be trusted and the adverse consequences of its lack or loss of trustworthiness. Spectacular failures in public trust in recent years have toppled industry giants and highlighted this vulnerability with exquisite clarity. Examples abound, with Enron, the largest bankruptcy reorganization to ever take place in the United States, "history's biggest financial fraud and its biggest audit failure" (Bratton 2002) being perhaps the most iconic of this century. The case against Enron and the auditing firm of Arthur Andersen focused on faulty recordkeeping and inappropriate destruction of records.

Rapid technological advances are fuelling trust requirements and concerns—and failures—more than ever before. The ability to conduct corporate or personal business electronically has promoted near-instant communication and removed geographic boundaries and associated costs of access to distant markets. The greater opportunities (and risks) deriving from new technologies have changed irrevocably business structures, but the fundamental issues affecting businesses remain: jurisdiction, validity and enforceability of agreements, and rights and obligations in transactions (Daughtery 2000). These issues arise in litigation, and the records of the business or individual tell the tale. But jurisprudence, whether considering the authority of legislation or the evolution of common law, is challenged by the very nature of these records created, maintained and used in digital form. It is not the substance of business conducted electronically that raises new questions, but the process, and it is in the creation, management and preservation of the records that this is realized (Daughtery 2000).

Records managers and archivists are dealing increasingly with digital materials. As keepers of society's records they must be confident that the trust in the records they tend is well placed and defensible. That confidence comes from the competencies they acquire through their professional training. Their education will need to be grounded in archival theory, tempered in legal concepts and adequate to manage the technological context of the records they acquire, appraise, describe,

produce for access and protect in perpetuity. As the form and substance of digital materials become increasingly complex, records professionals are looking to other disciplines for the tools that will enable them to carry out their traditional activities. Appraisal, acquisition and access in the digital age are mediated through technology. Always closely aligned with law, archival practice now turns also to tools of law enforcement. Digital forensics is moving beyond the realm of crime detection and prevention to assist records professionals to prove records' trustworthiness over time and across technological change.

This article begins with a brief discussion of technology and trust, and the components of trust required of records professionals in their role as trusted recordkeepers. It then touches on some of the recent developments in related disciplines that affect or assist the work of records professionals in order to lay the groundwork for an outline of a revised, interdisciplinary curriculum for masters of archival studies students and offers a preliminary look at the first such programme being developed at the School of Library, Archival and Information Studies (SLAIS) at the University of British Columbia (UBC). It is not the authors' intention to present a complete review of all relevant literature that is beyond the scope of the present article, but to introduce the concepts shared by domains of digital forensics, archival and diplomatic theory and records management practice in order to promote discussion and invite further research.

Technology and trust

Computers have been central to business technology since the last decades of the twentieth century. Early use of computers paralleled analogue business processes. Paper documents were scanned for quick reference and sharing, and born-digital documents were generally printed to paper for use and preservation. The challenges presented to records professionals by these digital records have been extensively researched since the early 1990s. Best practice for the creation, management and preservation of digital business records may not yet be *common* practice, but the knowledge exists. However, technological advances do not pause. The rapid development and widespread adoption of the Internet since the mid-1990s and the explosion of e-commerce conducted over the Internet have created a new wave of trust challenges for businesses, records and legal professionals alike. Business transactions are conducted on the Internet in one of four basic ways: by email, through chat rooms and listservs, through many and various World Wide Web interfaces, and through electronic document interchange, or EDI (Daughtery 2000). These transactions may be private, between two or more identified individuals, such as email. They may be visible to all members of a group, as are conversation threads on subscribed listservs or chat rooms. Or they may take place without the involvement of human agents, as in the case of automated computer-to-computer transmission (EDI). All these modes of exchange share the common feature of being paperless and lacking a physical signature (the traditional means of authentication). The identity of agents involved is revealed by the information an agent produces about itself (Daughtery

2000). All records so created may be subject to tampering and their identity and integrity questioned.

We trust what we know or what we believe others know. Disciplines that are concerned with the trustworthiness of records—notably law, history and diplomatics—have developed methods for testing record authenticity and reliability that are grounded in observational principles and rely on "a framework of inferences, generalisations, and probabilities" (MacNeil 2000, pp. 113, 115). Records on traditional media—paper, microfilm in modern bureaucracies—lend themselves to direct observation by which their authenticity and reliability can be examined and inferred. Digital records, in contrast, do not. The development of digital diplomatics (the application of the principles of diplomatics to digital records) has identified the necessary and sufficient attributes for authentic and reliable records created and maintained in complex, dynamic and interactive systems, many of which parallel traditional attributes of identity and integrity (Duranti 2005; Duranti and Preston 2008).

Signatures have been used for centuries to authenticate the documents upon which they appear. Merriam-Webster's *Dictionary of Law* (1996) defines a signature as "any mark (as initials, stamp, or printed name) made on a document and intended to serve as an indication of the party's execution or authentication of the document and intent to be bound by it." A signature identifies the signer and indicates her acceptance of the contents of the document and her willingness to enter into any agreement therein. In the digital world, no physical signature exists, and a complex encryption technology of digital signatures has developed to serve the same purpose. However, encryption alone does not verify that the parties involved are who they claim to be. To assure reliability of the parties' identities, digital signature technology relies on a trusted entity, or Certificate Authority, defined as "an independent, unbiased third party that contributes to, or provides, important security assurances that enhance the admissibility, enforceability and reliability of information in electronic form. In a public/private key system, a trusted entity registers a digitally signed data structure that binds an entity's name (or identity) with its public key" (Shamos 1999). Trust is thus established.

Technological solutions to the problem of trust in individuals and trustworthiness of records are not, by themselves, however, enough. Paul Toscano writes that "…encryption and security technologies alone cannot achieve the legal integrity of electronic documents, nor can they create or enhance an individual's expectations of privacy in personal and sensitive information" (Toscano 2000). To guarantee the authenticity and reliability of records requires a framework of policies, procedures, technologies, and intentional action or intervention by trusted entities—juridical persons imbued with accountability to the records. The concept of "trusted third-party recordkeeper" was developed in the context of electronic contracting and refers to a physical or juridical person who is entrusted with the maintenance of the records of EDI partners (Reams et al. 1997, p. 37). The InterPARES Project defined a "trusted custodian" in a similar way, as a neutral third party who has the knowledge required for attesting to and ensuring the continuing authenticity of the records (Duranti 2005, p. 21; Duranti and Preston 2008, pp. 709, 713). The involvement of trusted entities

responsible for creation, verification, authentication or preservation is necessary throughout a record's life cycle.

Educating for trust

Inspired by the sociological approach to the concept of trust, in her article "Trusting Archivists", Jennifer Borland writes that "[t]he rules of trust refer to those who give trust, as well as to those who receive trust; *trusters* [givers] and *trustees* [receivers]" (Sztompka 1999, p. 66 quoted in Borland 2009, p. 98). In the archival context, for the relationship between the giver of trust or *truster* (i.e. creator and/or society) and the receiver of trust or *trustee* (i.e. records manager, and/or archivist and archival institution) to be formed and thus considered trustworthy, the trust bond must be based on the following characteristics: *reputation*, which results from an evaluation of the trustee's past actions and conduct; *performance*, which is the relationship between the trustee's present actions and the conduct required to fulfil his or her current responsibilities as specified by the truster; c*onfidence*, which is an assurance of expectation of action and conduct the truster has in the trustee; and c*ompetence*, which consists of having the knowledge, skills, talents, and traits required to be able to perform a task to any given standard. "Competence is perhaps *the* most critical element for trust. Without competence, the trustee would not have been placed in a trust-relationship, as the trustee would not have the capability to fulfil the related responsibilities. Further, unless the responsibilities were fulfilled, reputation, performance and confidence could not exist to be measured" (Borland 2009, p. 98). Therefore, competence underpins all other elements of trust; in other words, trust is primarily based on competence, and competence is in large part provided by education.

In order to define what kind of education would contribute to qualifying records professionals as competent, it is necessary to identify the components of the "performance" that records creators and society at large expect of them. The InterPARES project, consistently with a variety of other research projects, has established that, in today's digital environment, all records professionals, regardless of the part of the records life cycle they are responsible for, in addition to their traditional educational armour, should possess knowledge on:

- how digital systems should be designed to create and maintain and/or preserve trustworthy digital records that can be regarded as material evidence of facts and acts, serving at the same time transparency, accountability (both administrative and historical) and the needs of a large variety of users;
- how the authenticity of digital records at any time during their life cycle can be presumed on the basis of circumstantial or environmental evidence, and how it can be verified when its presumption is weak;
- how records can be reliably extracted from the hardware or the systems in which they reside, identified, acquired and maintained in long-term storage in such a way that their authenticity can be presumed;
- how records should be authentically reproduced in the course of their long-term preservation;

- how the features of the records, the actions conducted over them, and the changes caused by such actions should be documented so that the requirements of quality assurance can be met;
- how forensic readiness should be established to meet the needs of e-discovery, and how the records submitted to court in evidence should be kept during and after the conclusion of court proceedings for as long as needed, so that they remain trustworthy;
- how long-term preservation activities can be conducted so that they would not interfere with the applicability of the business records exception to the hearsay rule;
- how the rights of all the parties involved (economic, intellectual, and moral) can be protected in the course of the processes of creation, management, acquisition and preservation; and
- how digital records and data that are scheduled for disposition must be handled to ensure destruction.

These competences qualify recordkeepers as "agents of accountability" able to fill specific roles.

In her exploration of the relationship between recordkeeping and accountability, Sue McKemmish has identified recordkeeping functions beyond implementation of good recordkeeping requirements (McKemmish et al. 2005, p. 237). This range of roles encompasses specification of requirements for records and systems, implementation, monitoring and enforcing. All four of these functions must be met in order to ensure accountability and inspire trust.

It is clear from this list of responsibilities that the challenges presented by managing digital records through time are ones that records professionals should not meet in isolation. If records are the "material evidences" of actions and events (Jenkinson 1947/1980, p. 246), then we need to protect them as such, building research alliances that foster the development of new knowledge that can support the role of trusted keepers of the authentic record of our times, which we claim. The knowledge base for records professionals is of course grounded in archival science and diplomatics, but it does not exist in a vacuum. As long ago as 1817, the archivist of Venice, Michele Battagia, observed that "archivists keep close relationships with governments, culture and the interests of the entire society" (Battagia 1817, p. 30, quoted in Duranti 2007, p. 47). He could have been speaking of the records professionals of today. Ethics, politics, law and administration, and an understanding of the fundamentals of digital technology as well as a solid grounding in archival theory all contribute to the formation of a professional with the competences necessary to rise to today's challenges. The model of education that this suggests is an interdisciplinary one.

The need for interdisciplinary knowledge to understand and manage the complexities of digital records has been expressed by experts in disciplines complementary to but distinct from archives and records management. Records-specific knowledge requirements have been articulated in particular in related disciplines of law, digital forensics, information assurance and cyber-security. Interdisciplinary alliances are beginning to form. In the next section of this article, the authors outline some of the convergences that are developing.

Law

> …virtually all evidence brought before a court within the next 3 years will be from a digital source (Mason 2007).

The Hon. John M. Facciola, United States Magistrate Judge, Washington DC, has proposed a new curriculum for law students in the United States that would address the challenges they are facing with respect to digital evidence. He calls for a radical reorganization that recognizes the meaninglessness of separating notions of "civil procedure," "judgments," and "evidence" when considering digital record creation, transmission, use, preservation and privilege.

> As I lectured … on the impact that the developments in information technology were having on items that fall uncomfortably within the rubric of "electronic discovery", I realized that I was making a terrible hash of the traditional law school curriculum… I felt that I was doing a jigsaw puzzle with the wrong pieces, and I wondered if a more conceptual approach would make more sense (Facciola 2010).

Facciola calls for instruction in the creation of electronic information, its use, retention and preservation, its transmittal and use in the resolution of disputes or in the assertion of governmental power in an administrative or criminal context. Although these sound very much like topics covered in a programme of education for archivists, he frames them in a legal context, linking them to topics relevant to a legal curriculum such as patent and copyright law as they pertain to the creation of electronic information, or tort actions based on electronic communication. He links preservation to the laws pertaining to privacy of information that is maintained and the consequences of its breach. He suggests examination of disposition and destruction in the context of cross-jurisdictional requirements and the consequences of the breach of those laws. With respect to transmission, Facciola focuses on security breaches, both criminal and in the context of investigation, including wiretaps and other seizures of all forms of electronic transmission to gather evidence of a crime, and finishes by suggesting a technical discussion of search capabilities, questions of privilege and how it is to be asserted, and a discussion of the significance of the new Federal Rule of Evidence 502. Without a return from the dead by Leonardo da Vinci, Facciola recognizes that "there is no modern polymath who could possibly teach all of these topics" and he calls for an interdisciplinary and team-teaching approach by competent authorities (Facciola 2010).

Facciola is by no means a lone voice in the legal profession calling for an interdisciplinary approach to records management and legal issues. Stephen Mason, editor of the *Digital Evidence and Electronic Signature Law Review*, predicts "rough justice" from a "collective failure of the legal system: by the prosecution, defence and judge," if lawyers and judges "fail to grasp that they need to begin to understand the attributes of evidence in digital format." Furthermore, he finds complicit in this potential failure "the majority of universities and law schools across the world to incorporate any discussion of digital evidence into the curriculum" (Mason 2007).

George Paul, in his seminal *Foundations of Digital Evidence*, identified the problems posed by digital technology to the understanding and evaluation of digital records offered in evidence (Paul 2008). He seeks to "lay a foundation for core competencies" essential for legal professionals to understand digital records and successfully do their jobs (Paul 2008, p. 16). These core competencies are the grist of archival education—the nature of digital records, their authenticity, integrity, identity and the concept of "original". The Sedona Conference is another influential voice for change, developing principles, guidelines and best practices, and offering continuing education for legal professionals, particularly in the area of e-discovery and electronically stored information (www.thesedonaconference.org).

Digital forensics

The practice of digital forensics is firmly rooted in computer science, and there are many articles and books by practitioners devoted to the development and testing of investigation techniques, issues and toolkits. However, there is a growing body of literature that focuses on more abstract theoretical questions of how digital forensics addresses authenticity, reliability and evidentiary potential of digital materials extracted or recovered from their native systems (see for example Palmer 2001; Mocas 2004). "When contemplation is codified in disciplined study, we have the sense of theory as that part of a technical subject devoted to elucidating the general facts, principles, or propositions on which the subject depends, as distinguished from the practice of it" (Eastwood 1994, p. 124).

The literature reveals a growing acknowledgement of the interdisciplinarity of digital forensic activities. The discipline of digital forensics has grown out of practice rather than theoretical concepts. It is first and foremost associated with the domain of law enforcement. The judicial system relies on the expert knowledge and testimony of digital forensics specialists for collecting and analysing electronically stored information (ESI) and extracting evidence for use at trial. The primary objective is prosecution, and forensic activity focuses on acquisition or recovery of existing material. "The criteria that define suitability for forensic evidence in this area are the most clearly defined since computer forensic analysis must follow the same longstanding statutory and regulatory guidelines imposed on other, more traditional forensic disciplines" (Palmer 2001, p. 4). Digital forensics is also at the core of the information assurance industry, serving military operations, business and industry in a real time environment. Its primary objectives are continuity of operations and availability of service (Palmer 2001, p. 3). Forensic techniques are also becoming more widely used in enterprise risk management (see for example Casey 2007, pp. 49–50; Rowlingson 2004, pp. 1–28; Ryan and Ryan 1995).

Eugene Spafford presented the "Big Computer Forensics Challenges" at the first Digital Forensics Research Workshop (DFRWS) in 2001 (Palmer 2001). Spafford called for a "full-spectrum" approach that does not rest on technology alone. Research is needed not only in the technology of forensic tools but also in the procedural, social and legal realms to create a holistic body of knowledge that both informs and supports the primary objectives of forensic analysis and leads to an integration of "forensic hooks" into live computer and network systems and away

from the "current band aid approach that produces point solution tools". Lack of standardization of analytical procedures, protocols and terminology; issues of accuracy, efficiency and retention of extracted material; the conflict between individual privacy rights and data collection requirements are all holding the development of the profession back. "We need to know how much information and what type, exactly, we must collect to afford the most accurate analysis under particular circumstances" (Palmer 2001, p. 7).

To place digital forensics in the framework of technical, procedural, social and legal realms one must look outside the technical discipline for complementary knowledge. The interdisciplinary nature of computer forensics is well established. The DFRWS *Road Map* identifies core competencies required from computer science, engineering sciences, material sciences, physics, mathematics, criminal justice, psychology, sociology and the existing forensic sciences.

Several areas are also identified in the *Road Map* as candidates for applicable specialization, including some that overlap with archival and diplomatic knowledge: languages/linguistics, image analysis and evidence preservation (Palmer 2001, p. 19). The literature that explores interdisciplinary possibilities expands the boundaries of traditional computer forensics, identifying needs for further research. Alastair Irons, for example, makes explicit the parallels and complementarities of digital forensics and records management in his analysis of the principles of computer forensics in the context of record characteristics of authenticity, reliability, integrity and usability (Irons 2006, pp. 102–112).

If digital forensics specialists are just discovering archival science, archivists have known for some time of their affinity to the forensic discipline. "If the historian is the lawyer in the court of history, then the archivist is the forensic scientist," wrote Elizabeth Diamond over 15 years ago. She notes the parallels between the two disciplines: each has the job of acquiring, preserving, arranging and making accessible "impartial evidence" and to clarify the meaning of that evidence through "its own distinct knowledge and methodology" (Diamond 1994, p. 140).

Information assurance and forensic readiness

The working definition proposed by the DFRWS in 2001 stated that digital forensic science is "[t]he use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations" (Palmer 2001, p. 17). The first part of this definition clearly relates digital forensics to its original function in law enforcement. Digital forensics in this capacity is reactive, acting on created materials. The second part of the definition opens the door to its proactive capacity to anticipate threats and disruptions. The DFRWS was quick to point out that digital forensics is a tool with applications in information assurance, but they cautioned, "Digital Forensic Science is not in the business of protection" (Palmer 2001, p. 17).

This anticipatory forensic endeavour, however, is increasingly capturing the effort and imagination of forensic discourse in the field of information assurance. The concept of forensic readiness, defined as the ability to maximize an organization's potential to use digital evidence while minimizing the cost of an investigation (Rowlingson 2004), emphasizes prevention and detection over post-incident investigation. Rowlingson outlines ten steps to enterprise forensic readiness that bear close resemblance to an implementation plan for a systematic records management programme. Although he does not provide a definition of digital evidence, business records are clearly a subset of the digital material to which he refers:

> Digital evidence is required whenever it can be used to support a legal process. … To succeed in a legal process, it is therefore essential that the organization has actively gathered the evidence it is likely to require. Moreover, it is vital to have the capability to process evidence cost-effectively, and to have suitably trained staff who know how to ensure potential evidence is preserved (Rowlingson 2004, p. 3).

A well-organized records management programme ensures that human-generated business records, at least, will meet these requirements.

Rowlingson continues to outline a plan for forensic readiness that parallels that of a records management programme (although he does not draw the comparison). He states that forensic readiness can add value to such activities as business continuity planning and should be mandated by senior management. Activities necessary to implement forensic readiness include:

- Updates to policies;
- Improvements in training;
- Systematic gathering of potential evidence;
- Secure storage of potential evidence;
- Preparation for incidents;
- Enhanced capability for evidence retrieval;
- Legal advice;
- Developing an in-house DFI capability, if required (Rowlingson 2004, p. 6).

It is not within the scope of this article to draw the parallels between records management and forensic readiness further, although one final link is worthy of note. Many of the questions associated with appraisal and description and with diplomatic analysis are found in questions Rowlingson poses as part of the process of evidence identification:

- Where is data generated?
- What format is it in?
- For how long is it stored?
- How is it currently controlled, secured and managed?
- Who has access to the data?
- How much is produced?
- Is it archived? If so where and for how long?

- How much is reviewed?
- What additional evidence sources could be enabled?
- Who is responsible for this data?
- Who is the formal owner of the data?
- How could it be made available to an investigation?
- To what business processes does it relate?
- Does it contain personal information?

The similarities between records management and digital forensics have not gone unnoticed, but have as yet not been explored in depth. Irons calls computer forensics and records management "compatible disciplines" and notes their mutual benefit, but states "[t]here remains very little published on the discussion of the potential implications of computer forensics for records managers or how computer forensics can enhance the records management discipline" (Irons 2006, pp. 109–110). Most of his arguments present the benefits of digital forensics to records management, although he does recognize at the end of his paper that many skills of records management—metadata expertise, functional requirements, retention and disposition, digital preservation, and so on—can benefit forensic investigative techniques. Perhaps more interestingly, he suggests that computer forensics could benefit from the application of theoretical models of records management.

Barbara Endicott-Popovsky and Deborah Frincke recognize that the "full-spectrum" approach called for in 2001 has still not been realized. Research has focused on forensic methods, tools and techniques, mainly from the perspective of law enforcement, and largely ignored a conceptual framework for proactive approaches. Endicott-Popovsky and Frincke propose to integrate investigative skills into network systems, effectively embedding forensic tools into live networks. Forensic readiness demands more than restoration of compromised systems, adding "augmented cognition capabilities" to network administrators. By incorporating security across the system development life cycle, evidence can be protected by embedding compliance mechanisms, reliability mechanisms and chain of custody procedures (Endicott-Popovsky and Frincke 2007, pp. 367–369). There are parallels between the concept of embedding security in network systems in order to protect the evidentiary capacity of digital objects and the concept of ensuring the capacity for digital records preservation at the time of creation. In order to maintain and preserve the authenticity and reliability (and therefore the evidentiary capacity) of digital records, the ability to preserve must be built into records from the beginning of their life cycle. A life cycle methodology applies to both forensic and digital preservation.

The contribution of records management and archival principles to digital forensics practices can be clearly seen in the discussion of digital evidence maps. With the advent in December 2006 of amendments to the United States Federal Rules of Civil Procedure (US Fed. R. Civ. P. 26(a)(1)(B)) including a mandatory duty of disclosure of all sources of digital evidence at the beginning of a civil dispute, organizations must be able to identify the source and location of all electronically stored information. However, IT experts, who are being asked to develop comprehensive data maps, are typically concerned with network

performance and security and "are not trained to think about IT systems as a source of evidence, develop strategies to locate unknown data sources, or provide expert testimony" (Casey 2007, p. 1). Records managers, in contrast, are trained to consider records as a source of evidence, develop strategies to maintain and preserve that evidence, and speak to its reliability and authenticity.

Digital forensics and cultural heritage

Digital forensics tools and techniques are also beginning to emerge as essential parts of the technical arsenal in cultural heritage institutions. While digital forensics in traditional fields of law enforcement and security operates at the cutting edge of technology, digital forensics in the cultural heritage community is being used retrospectively. Artists, writers, musicians, government officials, politicians, scholars, and other public figures are using digital technologies to create and communicate, and their *oeuvres* are arriving at libraries and archives on a variety of storage media. Some of these media may be obsolete, some may be contemporary, but all must be identified, and their contents extracted, arranged, described, preserved and made available within the constraints of privacy and access restrictions.

Archivists are using forensic tools to approach some of the key issues and challenges presented by born-digital cultural materials, including how to preserve the integrity of the materials, how to create and capture authentic digital copies and offer access to researchers that preserves the look and feel of the material as it was originally formatted. Forensic tools offer the possibility of preserving not only the finished documents and records of the creator but also evidence of how that creator worked, through recovery and preservation of, for example, browser logs, or workflow and productivity tools.[1] At the same time, forensic tools present the archivist with the capacity to recover deleted files or access material that the creator never intended to become available to researchers or the public, creating new ethical questions and concerns about the nature of private versus public.

The importance of digital forensics as a resource for keepers of our documentary heritage is detailed in the report of a project collaboration, recently completed, between the University of Maryland, the Bodleian Library and the Harry Ransom Centre at the University of Texas, Austin. The authors outline the benefits of incorporating digital forensic tools and techniques into archival workflows, including increased efficiency of information capture, preservation of integrity, greater capacity for analysis and documentation at all layers of abstraction, and identification of privacy issues. They end their report with a series of "next steps," which highlight the need for the development of networks for collaboration, interdisciplinary research and publication, and education and training that augments

[1] The Salman Rushdie Archive at Emory University is perhaps the best-known example. Emory provides researchers with the experience of sitting at Rushdie's computer and experiencing how he worked through emulation of his computer environment. See "Preserving Salman Rushdie's Digital Life," YouTube, http://www.youtube.com/user/emorylibraries#p/c/2/b1yrFlZo7wY. Accessed 11 March 2011.

traditional archival knowledge with basic competence in IT and digital forensic techniques (Kirschenbaum et al. 2010, pp. 62–64).

Digital records forensics—a new course of study

Educating records professionals for trust in the digital environment, then, is going to require the collaboration of experts from a variety of disciplines. One interdisciplinary alliance is being built through the intentional efforts of the Digital Records Forensics project (DRF). This collaborative joint research endeavour is the shared work of UBC SLAIS, the UBC Faculty of Law and the Vancouver Police Department (www.digitalrecordsforensics.org).[2]

The DRF project embraces the convergence of digital forensics, archival science and diplomatics in order to research and develop concepts and methods that will allow the records management, archival, legal, judicial and law enforcement professions to recognize records among all kinds of digital objects produced by digital technologies once they have been removed from the original system; to develop concepts and methods for determining the authenticity of records no longer in the original system and/or in the original format; to develop methods for maintaining records acquired from crime scenes or created by police to pursue crime over the long term so that their authenticity will not be questioned; and to develop the theoretical and methodological content of a new discipline, called "*Digital Records Forensics*", resulting from an integration of archival diplomatics,[3] computer forensics and the law of evidence with the project's newly developed knowledge. The project is unique in that it aims to develop new knowledge both by research and by bringing the research findings, as well as selected areas of knowledge of digital forensics, into the classroom, and letting this interaction produce new concepts, methods and practices.

The DRF research began by drawing the connection between diplomatics, the first forensic science developed in the western world, and digital forensics. Rather than resort to classical diplomatics, the DRF research took the concepts developed for the purpose of understanding and controlling digital records in the course of the InterPARES research (Duranti and Thibodeau 2006) and compared them to the corresponding concepts in digital forensics (Duranti 2009). The comparison clearly showed a fundamental similarity between the two conceptualizations of the notions of *record* and *trustworthiness*, but while the diplomatic concept of record is much more sophisticated than the forensic one and would certainly enrich the forensic

[2] The Digital Records Forensics project (2008–2011) is funded by the Social Sciences and Humanities Research Council (SSHRC) of Canada.

[3] Diplomatics developed originally in the seventeenth century as a science to establish the authenticity of mediaeval documents. Archival scholars have applied the principles and concepts of diplomatics in the twentieth century to modern documents, most recently digital documents. Archival diplomatics is the integration of archival and diplomatic theory about the contexts of creation, intrinsic and extrinsic elements, and transmission of documents; their relationship with the facts represented in them, and with other documents produced in the course of the same function and activities (Duranti 1998; Duranti and Thibodeau 2006; Duranti 2009).

body of theory, the forensic concept of trustworthiness, although lacking a clear theoretical distinction between reliability, authenticity, accuracy and authentication, is much more nuanced when it comes to authenticity, authentication and integrity.

Digital forensics, for example, differentiates data integrity from copy integrity, computer integrity and system integrity and has developed rigorous processes for assessing each, based on principles, such as those of non-interference and identifiable interference, repeatability, verifiability, objectivity and transparency. This intellectual framework for integrity can be extremely useful to records professionals to design proper processes of identification, acquisition, characterization, reproduction and migration of the records for which they are responsible. In another example, the relationship identified by digital forensics between authenticity and chain of continuity or of legitimate custody, based on a lack of trusted technological means of authentication, can be an eye opener for many digital archivists. And more, the distinction between a copy and an image made by forensic experts, if adopted by archivists, would ensure that we do not infringe rights to privacy and copyright when acquiring archival material. Finally, the very tight, detailed, and rigorous workflow for the extraction of records from the systems and/or hardware in which they reside to their storage in a trusted repository is something that could give reliability to the archivists' procedures of acquisition.

Digital records forensics sits at the nexus in a sphere of complementary disciplines that can contribute to solutions to these procedural, social and legal challenges.

This representation (Fig. 1) shows traditional sources of digital forensics knowledge and influence in the bottom and right hand categories, but also recognizes the potential contribution of knowledge from archival science and diplomatics, and records and information management. One can infer the relevance of these knowledge sources from questions posed by digital forensics practitioners about the trustworthiness of digital evidence (Kirschenbaum et al. 2010),[4] reliability (see for example Carrier 2003),[5] and authenticity and authentication (Kabay 2009).

Throughout the period of the research, the DRF project has developed an interdisciplinary bibliographic database, a case law registry, and a terminology database that allows for a comparison of terms and concepts. These resources are tested as educational instruments by all participants in the research, the UBC Archival Master's and PhD programmes, the UBC Faculty of Law, the University of Washington Information Assurance and Cybersecurity programme in the School of Information, and the Computer Forensics and Identification Divisions of the Vancouver Police Department. In the fall of 2012, we will begin to test these

[4] The second workshop of the DFRWS 2001 symposium was entitled "The Trustworthiness of Digital Evidence," and posed the questions, "Is the abstract, transformed nature of digital data troublesome in terms of integrity and fidelity when viewed as evidence? If so, can it be overcome?"

[5] Carrier states that digital forensic tools (at the time of writing) provide access to evidence, but do not offer the means to determine that evidence's reliability.

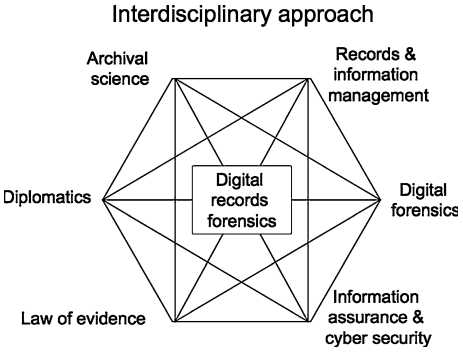


Fig. 1 An Interdisciplinary approach to digital records forensics

resources in the context of a new stream of study in the Master of Archival Studies (MAS) programme in UBC SLAIS, imparting the interdisciplinary knowledge developed so far in the context of a records forensics specialization within the archival programme. Students training to be archivists and records managers who choose this stream will have an opportunity to go beyond the core required courses in archival diplomatics, digital diplomatics and the preservation of digital records and explore in more depth the intersection between digital forensics, digital records management and preservation, and law.

In partnership with the School of Information at the University of Washington, the new stream will offer courses aimed at providing competence in the creation, keeping and preservation of authentic digital records by combining concepts, methods and practices from:

- diplomatics (and specifically digital diplomatics), which embodies the theory of the record and record making;
- digital forensics, which comprises the core concepts and methodologies related to the acquisition, identification, analysis and evaluation of digital materials, and the related practices;
- the law of evidence, which establishes rigorous parameters for quality assurance of systems and forensic readiness of records management programmes;
- archival science, which provides the theoretical and methodological knowledge related to digital recordkeeping and long-term digital preservation;
- information technology, which offers the necessary understanding of systems concepts, computer architecture, computer network communication, discrete mathematics, database design, algorithms and data structures, imperative programming, markup languages and end-user programming tools; and
- organizational information assurance, which examines concepts, elements, strategies, skills related to the life cycle of information assurance, involving policies, practices, mechanisms, dissemination and validation that ensure the confidentiality, integrity and availability of information and information systems. This includes consideration of "forensic readiness" or maximizing the collection of credible digital evidence while minimizing the cost of incident response (Tan 2001).

The new stream, consistent with the rest of the archival programme, is grounded in three educational principles: (1) the acquisition of core theoretical and methodological knowledge of the discipline(s); (2) education situated in the local context of the specific, relevant juridical-administrative environment as well as the global context of international standards; and (3) the value of scholarly and practical work. Research, a critical expression of the intellectual nature of the study and the scholarly substance of the work that professionals do, will be an essential part of the programme. It will be this engagement in research that will produce new knowledge and support the creation of dedicated full-fledged programmes in Digital Records Forensics. Graduate programmes are judged to a significant degree by the quality and quantity of the research produced by faculty and students; thus, expanding the opportunities for research is vital to their success and growth. Experiential learning in the context of the education of professionals is not an exercise to discover theory and methods empirically. Its main purpose is to provide future professionals with a way of applying the theoretical and methodological knowledge learnt in class and testing it in the professional arena. This is the best way of demonstrating to the students that theory and practice feed each other and neither could have value without the other. Recently, some programmes have introduced co-operative work experience opportunities for their students. Co-operative education is a learning method that, through pre-employment workshops, coaching by career specialists and workplace experiences, offers students the opportunity to combine real world experience with their classroom education and develop employment skills specific to the records professions. Simply stated, universities and employers co-operate to provide students with an opportunity to learn in a workplace setting by alternating practical, paid work experience in various fields of interest with their academic studies. Most importantly, in the first stage of stream development, the practical experience would allow digital records forensics students and their professors to assess the value of their education, to identify gaps and to work towards a course and curriculum development that better serves the needs of professionals. At the same time, the students and their programme of education would be visible to professionals, who will appreciate the value of both and generate the demand required by universities to support such programmes (Duranti and Endicott-Popovsky 2010).

The need to support the archivist's role as trustee of digital materials, whether evidence collected in the pursuit of justice or heritage materials supporting societal memory, with the proper competences requires looking beyond traditional education to team up with the most improbable allies to educate for trust. It is difficult for any archival programme to impart all this knowledge on its own, but alliances can be built, and student and faculty exchanges can be organized, as is happening between the UBC and the University of Washington. Graduate programmes in digital records forensics would not undermine or substitute more traditional programmes in archival science, but augment them with a very particular knowledge base. As Mark Pollitt has written about the future of digital forensics practice, it is no longer a linear process of data recovery, but "an evidence-based knowledge management process" requiring interdisciplinary teamwork (Pollitt 2010). We believe archivists and records managers also have a place on the team.

References

Battagia M (1817) Discorso sull'antichità ed utilità' degli archivi, nonch è su la dignità degli archivisti. Tipografia di Alvisopoli, Venezia

Bodleian Library futureArch Blog (2011) http://futurearchives.blogspot.com/. Accessed 20 June 2011

Borland J (2009) Trusting archivists. Archivi & Comput XIX(1):96–109

Bratton WW (2002) Enron and the dark side of shareholder value. Tulane Law Rev 5–6:1275–1362

British Library, Digital Lives Project (2011) http://www.bl.uk/digital-lives/. Accessed 20 June 2011

Carrier B (2003) Defining digital forensic examination and analysis tools using abstraction layers. Int J Digit Evidence 1(4):1–12. www.ijde.org. Accessed 20 June 2011

Casey E (2007) What does "forensically sound" really mean? Digit Investigation 4(2):49–50. http://www.sciencedirect.com/science/article/B7CW4-4NWNCSP-1/2/36717bc8a1dc225cfec6a4c835866999. Accessed 20 June 2011

Daughtery WH Jr (2000) Adapting contract law to accommodate electronic contracts: overview and suggestions. Rutgers Comput Technol Law J. http://www.accessmylibrary.com/article-1G1-65865452/adapting-contract-law-accommodate.html. Accessed 20 June 2011

Diamond E (1994) The archivist as forensic scientist–seeing ourselves in a different way. Archivaria 38:139–154

Digital Records Forensics Project (2011) http://digitalrecordsforensics.org/. Accessed 20 June 2011

Duranti L (1998) Diplomatics: new uses for an old science. Scarecrow Press, Lanham

Duranti L (ed) (2005) The long-term preservation of authentic electronic records: Findings of the InterPARES Project Archilab, San Miniato

Duranti L (2007) Models of archival education: four, two, one, or a thousand? Archives & social studies. A J Interdisciplinary Res 1(1):1–21

Duranti L (2009) From digital diplomatics to digital records forensics. Archivaria 68:39–66

Duranti L, Endicott-Popovsky B (2010) Digital records forensics: a new science and academic program for forensic readiness. J Digit Forensics, Security and Law 5(2):1–12. http://www.jdfsl.org/subscriptions/JDFSL-V5N2-Duranti.pdf

Duranti L, Preston R (eds) (2008) A framework of principles for the development of policies, strategies and standards for the long-term preservation of digital records. InterPARES 2: Interactive, dynamic and experiential records. ANAI, Padova. http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_appendix_19.pdf. Accessed 20 June 2011

Duranti L, Thibodeau K (2006) The concept of record in interactive, experiential and dynamic environments: the view of InterPARES. Arch Sci 6(1):13–68

Eastwood T (1994) What is archival theory and why is it important? Archivaria 37(Spring):122–130

Endicott-Popovsky B, Frincke D (2007) Embedding Hercule Poirot in networks: addressing inefficiencies in digital forensic investigations. Foundations of Augmented Cognition, pp 367–369. http://dx.doi.org/10.1007/978-3-540-73216-7_41. Accessed 20 June 2011

Facciola JM (2010) Explosions and eruptions: some thoughts on a conceptual approach to law school and post-graduate education. EDDE J 1:1. http://new.abanet.org/sections/scitech/ST203001/PublicDocuments/EDDE%20Journal%20-%20volume%201%20issue%201.pdf. Accessed 20 June 2011

Irons A (2006) Computer forensics and records management – compatible disciplines. Records Manag J 16(2):102–112. http://www.emeraldinsight.com/10.1108/09565690610677463. Accessed 20 June 2011

Jenkinson H (1947) The English archivist: a new profession. In: Ellis RH, Walne P (eds) (1980) The selected writings of Sir Hilary Jenkinson. Alan Sutton, Gloucester

Kabay ME (2009) The Parkerian Hexad. Powerpoint slides. http://www.mekabay.com/overviews/index.htm. Accessed 11 Apr 2010

Kirschenbaum M, Ovenden R, Redwine G (2010) Computer forensics & born digital content in cultural heritage collections. Council on Library and Information Resources, Washington

MacNeil H (2000) Trusting records: legal, historical, and diplomatic perspectives. Kluwer Academic Publishers, Dordrecht

Mason S (2007) Editorial. Digital evidence and electronic signature law review 4:2. http://www.deaeslr.org/2007.html. Accessed 20 June 2011

McKemmish S, Piggott M, Reed B, Upward F (eds) (2005) Archives: recordkeeping in society. Charles Sturt University, Wagga Wagga

Merriam-Webster's Dictionary of Law (1996). http://dictionary.lp.findlaw.com/dictionary.html. Accessed 20 June 2011

Mocas S (2004) Building theoretical underpinnings for digital forensics research. Digit Investigation 1(1):61–68. http://www.sciencedirect.com/science/article/B7CW4-4BMXXJS-C/2/9154d2932943f309d86f8a748ac40ab3. Accessed 20 June 2011

Palmer G (2001) A road map for digital forensics research. Technical report from the First digital forensics research workshop (DFRWS), technical report DTR-T001-01. Air Force Research Laboratory, Rome Research Site

Paul GL (2008) Foundations of digital evidence. American Bar Association, Chicago

Pollitt M (2010) A history of digital forensics. In Chow KP, Shenoi, S (eds) Advances in Digital Forensics VI. IFIP AICT 337:3–15

Reams BD Jr, Kutten LJ, Strehler AE (1997) Electronic contracting law: EDI and business transactions, 1996–1997 edn. New York

Rowlingson R (2004) A ten step process for forensic readiness. Int J Digit Evidence 2(3):1–28. www.ijde.org. Accessed 20 June 2011

Ryan DJ, Ryan JJCH (1995) Risk management and information security. http://danjryan.com/Risk.htm. Accessed 20 June 2011

Shamos MI (1999) Hyperdictionary of electronic commerce law. Institute for eCommerce. http://euro.ecom.cmu.edu/resources/elibrary/eclgloss.shtml. Accessed 20 June 2011

Sztompka P (1999) Trust. Cambridge University Press, Cambridge

Tan J (2001) Forensic readiness. @Stake, Cambridge, MA

Toscano P (2000) Toward an Architecture for the Virtual World. John Marshall J Comput Inf Law XIX(1). http://www.jcil.org/journal/articles/167.html. Accessed 3 August 2011

Author Biographies

Luciana Duranti is chair of the Master of Archival Studies at the School of Library, Archival and Information Studies of the University of British Columbia and a professor of archival theory, diplomatics and the management of digital records in both its master's and doctoral archival programmes. Dr. Duranti is presently project director of InterPARES (1999–2012), the largest research project on the long-term preservation of authentic electronic records; principal investigator in a research project entitled Digital Records Forensics (2008–2011); and co-investigator in a research project examining issues of copyright and long-term preservation in the context of universities institutional digital repositories (2009–2011). She is developing digital records guidelines for the UNESCO Memory of the World International Register and education modules for trusted digital records professionals for the International Council on Archives. She is active nationally and internationally in several archival associations and in boards and committees, such as the Italy's National Commission for Archives (2007–2013) and the UNESCO International Advisory Committee of the Memory of the World Programme (2007–2013) and has been the president of the Society of American Archivists (1998–1999), of which she is a fellow. She publishes widely on archival history and theory and on diplomatics.

Corinne Rogers is a doctoral student at the School of Library, Archival and Information Studies at the University of British Columbia. She holds an MA in Musicology from the University of Western Ontario and a Master of Archival Studies from UBC. Corinne is a graduate research assistant on InterPARES 3 and the Digital Records Forensics Project.