Authenticity of Digital Records: A Survey of Professional Practice / L'authenticité des documents numériques: Un survol des pratiques professionnelles

Corinne Rogers

Canadian Journal of Information and Library Science, Volume 39, Number 2, June juin 2015, pp. 97-113 (Article)

Published by University of Toronto Press
DOI: https://doi.org/10.1353/ils.2015.0015

The Canadian Journal of Information and Library Science

La Revue canadienne des sciences de l'information et de bibliothéconomie

Authenticity of Digital Records: A Survey of Professional Practice

L'authenticité des documents numériques : Un survol des pratiques professionnelles

Corinne Rogers
University of British Columbia
corinne.rogers@ubc.ca

Abstract: Authenticity of digital material is an enduring concern. However, while most people intuitively understand what authenticity is, few are able to identify exactly what is required to ensure, assess, and guarantee it. Heuristic and hermeneutic assessments of authenticity do not support any quantifiable measures of authenticity. Several important research projects have studied the means of ensuring that authenticity is protected throughout the life cycle of digital material, however, even as archival research and scholarship continue to offer insight into the nature of authentic digital objects and their preservation, new technologies, specifically distributed networked systems connected through the Internet, create new challenges to security and authenticity. This article reports on the author's research into the practices of records and information professionals to ensure, assess, and/or protect the authenticity of digital records and data.

Keywords: authenticity, trusting records, chain of preservation

Résumé : L'authenticité des matériaux numériques est une préoccupation qui dure. Mais alors que la plupart des gens comprennent intuitivement ce qu'est l'authenticité, peu sont en mesure d'identifier exactement ce qui est nécessaire pour assurer, évaluer et garantir l'authenticité. Les évaluations heuristiques et herméneutiques de l'authenticité n'appuient pas les mesures quantifiables de l'authenticité. Plusieurs projets de recherche importants ont étudié les moyens d'assurer que l'authenticité est protégée tout au long du cycle de vie du matériau numérique, cependant, tandis que la recherche d'archives et l'érudition continuent d'offrir une réflexion sur la nature des objets numériques authentiques et leur conservation, les nouvelles technologies, en particulier les systèmes distribués en réseau reliés par Internet, créent de nouveaux défis pour la sécurité et l'authenticité. Cet article rend compte de la recherche de l'auteur sur les pratiques documentaires des professionnels de l'information visant à assurer, évaluer, et/ou protéger l'authenticité des documents numériques et des données.

Mots-clés : authenticité, confiance aux documents, chaîne de conservation

Introduction

The digital universe is predicted to grow by 40 percent a year into the next decade, and businesses and governments are strategizing to take advantage of new opportunities afforded by digital information in its many and diverse forms

(Turner et al. 2014). Cloud computing offers significant economies of scale, and enterprises are rapidly moving, or considering moving, established computing practices, including digital records storage and management, to the cloud, where users relinquish a measure of control over the materials and technologies. Cloud computing now accounts for only 5 percent of total enterprise information technology (IT) spending, but this number is growing. As well as new technological infrastructure for traditional digital materials, we are entering the age of the "Third Platform," according to the International Data Corporation (IDC),[1] defined as "the next-generation compute platform that is accessed from mobile devices, utilizes Big Data, and is cloud based." Not all of the information created in the digital universe will be, or needs to be, preserved, but of the data and records that do warrant preservation, how will their authenticity be established and protected in these diverse and rapidly evolving technological contexts?

The 2014 IDC report states that maximizing opportunity requires certain imperatives for IT organizations but that "real transformation to a data-driven or software-defined enterprise is an "all-hands-on-deck imperative" not restricted to IT alone (Turner et al. 2014, 7). Those of us in records professions might well rejoice at this forecase. After all, much of the digital material being created by public and private sector organizations is in our purview to create, capture, manage, and preserve as records and data that form the foundation of business decisions and corporate and societal memory. Our professional codes of ethics hold us to principles of recordkeeping such as accountability, integrity, protection, compliance, availability, transparency, authenticity, preservation, security, protection, availability and use, privacy, and trust (Association of Canadian Archivists 1999; Society of American Archivists 2011; ARMA International 2014).

Preservation of trustworthy records regardless of medium—that is, records that can be proven authentic, reliable, and accurate—is at the core of the archival endeavour. It is about more than secure storage. Preservation encompasses all of the tools and techniques, policies, and procedures that ensure the target material remains trustworthy, accessible, and usable over time and across technological change. It requires the cooperation and collaboration of an inter-disciplinary team including archivists and records managers as well as IT professionals. In the digital universe, authenticity continues to be an enduring, if elusive, concern.

However, even though enterprises assume liability or responsibility for 85 percent of all data in the digital universe, the 2014 IDC report does not once mention issues of authenticity, trust, reliability, or integrity of this data. These qualities seem subsumed by the imperatives of security and privacy, the ability to enable and manage the explosive growth of mobile devices (and, presumably, the data they generate), and the ability to query data from wherever it may be stored (cross-boundary and cross-jurisdiction). Furthermore, the allocation of security budgets shows that prevention and protection from data breach and unauthorized access far outweighs money allocated to breach response (EMC Corporation 2013) and that the priority, in the event of a breach, is to restore service at the expense of the protection of trace evidence that would aid investigation (Endicott-Popovsky, Frincke, and Taylor 2007). If, as David Weinberger is often quoted, transparency is the new objectivity, then security is the new authenticity.

The professional discourse of archivists and records managers and the concerns for data in the information technology sector may overlap in the areas of privacy, access, and security. However, they too often occur as conversations rather than as collaborations. And while the trustworthiness of records and data may still be viewed by the enterprise as the responsibility of records professionals, the primacy of security often places IT ahead of records management. The authority of records professionals may be overshadowed or undermined by their reliance on IT for systems implementations as well as the focus on information and data analytics as business drivers (Richards 2014).

This article reports on the results of a survey of records professionals designed to explore their practices in ensuring and assessing the authenticity of records, documents, and data for which they are responsible. The survey is not limited to questions about the management of records and data in the cloud, and, in fact, most of the respondents are working primarily in the "Second Platform"—the distributed world of LAN/Internet and client/server architectures (EMC Corporation 2013). In 2013, less than 20 percent of the data in the digital universe was stored or processed in the cloud, but, by 2020, that figure is predicted to double. Understanding how authenticity is assessed and protected for digital records and data in current enterprise service architectures is foundational to understanding the challenges records professionals face in cloud platforms. If businesses and governments rely on information and data increasingly coming from third parties, mobile devices, and sensors, authenticity will continue to be a critical issue.

The issue of authenticity

Most people intuitively understand authenticity to be the quality of genuineness, but few are able to identify exactly what is required to ensure, assess, and guarantee it. Authenticity, the quality of a record that is what it purports to be, has historically been understood as deriving from the circumstances of a document's creation, if known, and from the manner and place of its preservation. The presence of a signature indicated the agreement of the author with the content of the document and authenticated the transaction recorded therein. Signatures of witnesses or countersigners further verified the document's authenticity. Signers and countersigners could be questioned if necessary, and their testimony used as a guarantee of genuineness. Such determination of authenticity was based on observation and testimony.

This understanding of authenticity, elegant in its simplicity if challenging to apply, is at the root of archival, diplomatic, and legal theory and has been codified in records management standards. According to archival science, record authenticity is "the trustworthiness of a record as a record, i.e. the quality of a record that is what it purports to be and that is free from tampering or corruption"

(InterPARES Glossary, n.d.). *Black's Law Dictionary* (n.d.) defines "authentic" as "Genuine; true; having the character and authority of an original; duly vested with all necessary formalities and legally attested; competent, credible, and reliable as evidence." The Society of American Archivists defines "authenticity" as "the quality of being genuine, not a counterfeit, and free from tampering, and is typically inferred from internal and external evidence, including its physical characteristics, structure, content, and context." This definition closely associates a record's authenticity with the creator of the record, something that can be verified by testing the physical and formal characteristics of the record. Authenticity as a record does not automatically imply reliability of the content of the record (Duranti 1998, 46; Pearce-Moses 2005). Finally, we see this concept of authenticity codified in ISO 15489, the international records management standard as follows:

> An authentic record is one that can be proven
> a. to be what it purports to be,
> b. to have been created or sent by the person purported to have created or sent it, and
> c. to have been created or sent at the time purported" (International Organization for Standardization 2001, s. 7.2.2).

In common law legal systems, documentary evidence must be authenticated to be admissible at trial. Authenticity, established through processes of authentication, is codified in our legal systems through statute and common law. Authentication of documentary evidence is accomplished through witness testimony, expert analysis, non-expert opinion, or, in the case of public documents or other special types, circumstances of record creation and preservation.[2]

These heuristics, based heavily on the appearance of documents, have developed over centuries and are still operational today, often misguidedly applied to digital documents. In interviews conducted in 2011 with lawyers, digital forensics experts, and records managers during the Digital Records Forensics Project (a three-year collaboration from April 2008 to April 2011 between the University of British Columbia's School of Library, Archival and Information Studies, the UBC Faculty of Law, and the Computer Forensics Division of the Vancouver Police Department), one respondent from the legal domain answered the question about determining the authenticity of documents: "You can tell just by looking at it" (Rogers 2011).

Authenticity is also contextual: "The meanings of 'authenticity' are relative to the concept of authentic that is held by different disciplines" (Lauriault et al. 2007, 140). This idea has been explored in recent literature (MacNeil and Mak 2007; Duncan 2009; Mak 2012). At the root of these explorations is the concept of authenticity as a social construction dependent on the context or discipline within which authenticity is defined, interpreted, and required. If we subscribe to the view that digital resources are "in a continuous state of becoming" as they are created, used, migrated, preserved, and accessed over time, then so too is the nature of their authenticity (MacNeil and Mak 2007, 26). In both cases, the questions remain about how to define the necessary elements of authenticity within a given context and how to assess them.

Much research has been conducted by records professionals on the nature of digital records and their attributes that may support the presumption of their authenticity. Still, current means of assessing authenticity do not offer any quantifiable measures. There is a pressing need for measures such as our financial, governmental, health, critical infrastructure, and social network systems to increasingly rely on complex integrated, interdependent (although not necessarily interoperable), distributed networked systems.

Digital technology's many benefits and challenges in respect of documentary material are well known. The benefits, including the ease of creation, search, access, and sharing, are offset by the ease of alteration, loss of integrity that may be difficult or impossible to detect, difficulty in establishing ownership and authorship, and difficulty in enforcing intellectual rights. The advent of cloud computing has increased the challenges, introducing, in particular, all of the issues arising from third party handling of material and jurisdictional questions about material created, stored, and transmitted around the globe, to name but two examples.

Records, defined as documents created or received in the course of practical activity and set aside for further action or reference, are the raw material of archival research and scholarship (Duranti 1993, 9; Eastwood 1994, 125; Duranti and Michetti 2015). In the digital environment, research agendas in information management communities focus on authenticity as an integral value that must be protected over time and across technological change through digital preservation (joining values of sustainability, accessibility, and understandability), broadening the scope of enquiry beyond records as narrowly defined by archival theory to documents, data, and digital objects of all types.

Archival science and the science of diplomatics have supported archivists in their understanding of the authenticity of traditional records. Authentic records are those whose identity can be established and whose integrity can demonstrated through an unbroken chain of custody over time. Diplomatics posits that all records can be analysed, understood, and evaluated in terms of a system of formal elements that are universal in application and decontextualized in nature (Duranti 1998). The InterPARES Project (International Research into Permanent Authentic Records in Electronic Systems, Phase 1 and 2), adopted the theoretical framework of diplomatics for the study of digital records and successfully developed the chain of preservation: "A system of controls that extends over the entire lifecycle of records and ensures their identity and integrity in any action that affects the way the records are represented in storage, or presented for use" (InterPARES Glossary, n.d.). The concept of a chain of preservation extends the controls implicit in the idea of chain of custody to address the susceptibility of digital records to corruption or loss. Requirements for establishing the authenticity of digital records are articulated in the benchmark requirements supporting the presumption of authenticity of electronic records and the baseline requirements supporting the production of authentic copies of electronic records (Duranti 2005b) and the Creator and Preserver Guidelines (Duranti and Preston 2008).

Digital diplomatics is ideally suited to the analysis of authenticity of digital records as defined by archival science, but it is limited when the subject of analysis is broadened to include digital objects that may not satisfy that precise, but narrow, definition (MacNeil and Gilliland-Swetland 2005, 52; Duranti and Endicott-Popovsky 2010, 2). Archivists are now creating research alliances with digital forensic practitioners to develop and extend the applicability of digital diplomatics in the field of digital preservation and the focus on authenticity, reliability, and accuracy (Duranti 2009; Kirschenbaum, Ovenden, and Redwine 2010; John 2012).

In the traditional environment, a record is presumed authentic if it is relied on by its creator for the conduct of business and maintained in an unbroken chain of custody by the creator or his legitimate successor(s) (Duranti 1997, 214; Eastwood 1994, 127). Archival documents, deemed authentic by virtue of the circumstances of their creation and maintenance as part of the aggregate of records unified by the archival bond, are also therefore presumed reliable and their contents accurate.

In the digital environment no such automatic presumption of authenticity should exist. Digital technology has upset the traditional systems of control that have ensured the creation of authentic records and the means of presuming their continued authenticity over time and across technological change (MacNeil and Gilliland-Swetland 2005, 21; Lauriault et al. 2007, 140). Digital records differ significantly from paper records. Records, documents, and data created and stored in computer media are volatile and subject to loss, intentional or unintentional alteration, contamination, or corruption, even when they are still in the custody of their creator. Their authorship, provenance, or chain of custody may be difficult or impossible to determine. They may be transmitted, shared, and copied with ease. Their accessibility is subject to hardware and software obsolescence and incompatibility. Even if the creator relies on a digital record in the course of business and maintains its unbroken chain of custody, the fragility and vulnerability of digital records demands explicit action to protect the record's authenticity. Furthermore, reliability and accuracy are no longer directly linked with authenticity and may be compromised together or separately (Duranti and MacNeil 1997, 48; Duranti 2005a, 1; MacNeil and Gilliland-Swetland 2005, 21; Duranti and Thibodeau 2006, 54).

Survey: indicators of authenticity

As part of a broader research project exploring concepts and practices of authenticity of digital records and data, the author conducted a web-based survey from 3 March to 1 May 2014. The purpose of the survey was to gather basic information about how records, information, or systems professionals ensure, assess, and/or protect digital records' authenticity, what metadata they employ or rely on, and what indicators of authenticity they consider to be important. The survey was posted on the major English-speaking archival and records management listservs.

It is my contention that despite large-scale, significant, and influential research into the topic of authenticity, primarily in the context of long-term preservation, the theoretical results of these projects are not being consistently applied in the practice of records professionals. This hypothesis is explored in the survey. The broad research questions motivating the survey interrogate notions of authenticity of digital records and data and investigate how records professionals interpret, ensure, and assess authenticity.

The survey consisted of seventeen questions, designed to explore work practice and belief about record authenticity. Demographic questions asked respondents to identify their job or position and the sector in which they work, their age, level of education, and discipline of their degree(s). Subsequent questions explored their main professional responsibilities, the means they used to ensure authenticity, what metadata they routinely applied or relied on for that purpose, whether they had ever been called upon to make a formal attestation of authenticity in a legal or administrative proceeding and, if so, what indicators had been most important in that attestation, and whether their organization explicitly defined authenticity in its policy instruments. The survey sought to explore the relationship between practice and belief—that is, what records professionals relied on in their work and whether that matched their belief or trust in authenticity indicators, identified from the perspective of archival science. It also sought to distinguish between what I have termed "social" and "technological" tasks and indicators of authenticity.

Social tasks are those conducted on the records or digital objects as conceptual objects, while social indicators of authenticity are instruments developed by an organization to support the creation, management, or preservation of records (for example, classification schemes, retention and disposition plans, and policies and procedures documents). They are based on domain knowledge and created and implemented by the intention of human actors (records professionals, management, legal counsel, and so on). They may or may not be present within a given organization; they may be mandatory or voluntary in their application or use, and, even when mandatory, they may be circumvented or adapted in practice. They include the foundational instruments of archival and records management practice: policy instruments, classification schemes or file plans, retention and disposition schedules, and archival description or other descriptive measures (which may be captured in varieties of descriptive metadata). Technological tasks treat the records as logical objects and involve technical aspects of preservation or curation, monitoring or enforcing security, or designing records systems. Technical indicators are non-discretionary in their creation—that is, they are the result of a work process or state change in the records (for example, system metadata capturing date created and date modified), are algorithmically generated or implemented by the technological components (for example, computer, network) of the overall record system (for instance, checksums, audit logs), are created to manage and control system access and security, or are created by a third party as specifications to a part of the technological system (for example, documentation about software). Technological indicators may be used to control the records but are more focused on controlling the system in which the records reside. They include audit logs, access controls and security measures, cryptographic validation techniques, and system metadata as well as technical documentation. These distinctions were explored in a series of ranking, Likert-style questions. They were further supported by open-ended opinion questions asking respondents to give their own definition of authenticity and identify the indicators they felt were most important.

Preliminary findings

The survey received 441 responses. Of these, 148 did not answer any questions beyond those gathering demographic information and were discarded. Of the remaining 293 responses, participants self-identified primarily as archivists (45 percent) and records or information managers (33 percent). The remaining 22 percent were split between information professionals (librarians, administrators, 10 percent), educators (6 percent), and other (6 percent). Industry sectors most represented were information and cultural industries (including libraries and archives, broadcast, and telecommunications) and government (see Figure 1). Industry sectors were condensed from the North American Industry Classification System (Statistics Canada and Standards Division 2012).

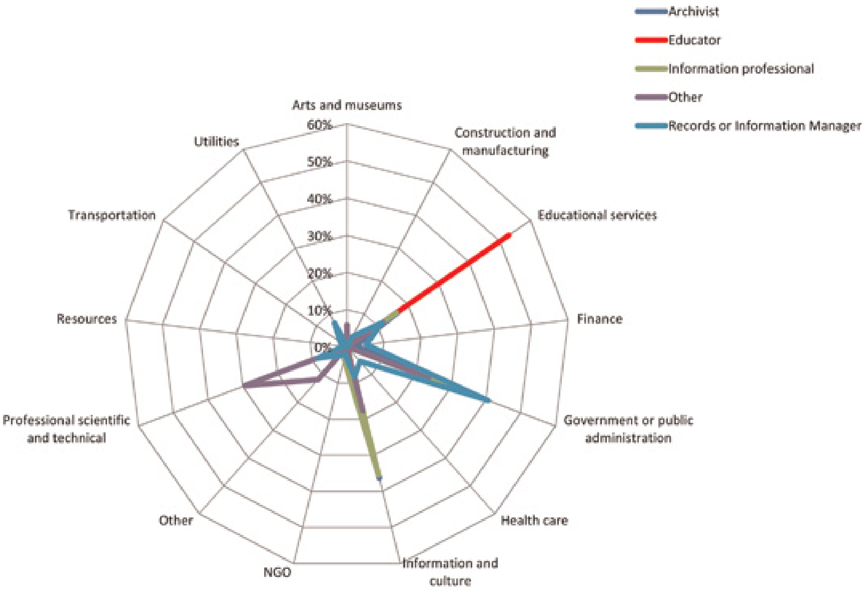

Figure 1: Respondents by profession and industry sector (n = 293)

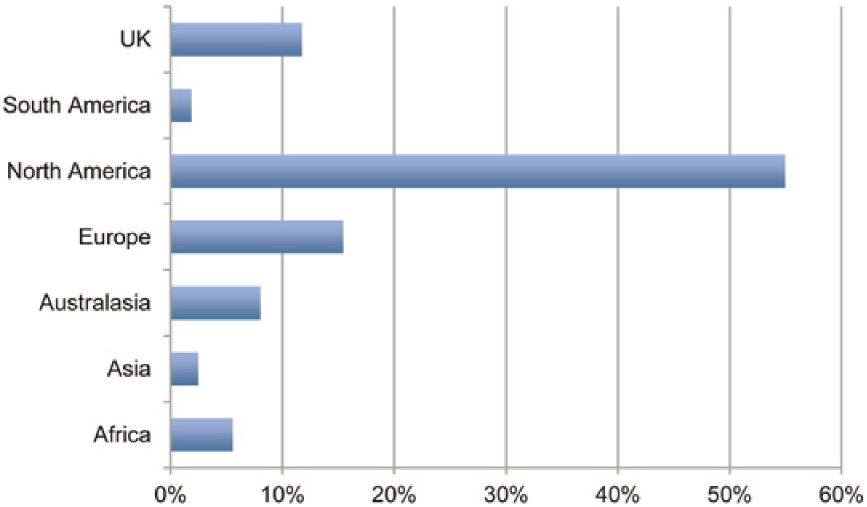

Figure 2: Percentage of respondents by continent

The survey achieved limited global reach, with the majority of respondents coming from North America (55 percent), followed by Europe (15 percent), and the United Kingdom (12 percent) (see Figure 2).

Respondents were asked a series of questions to determine their job responsibilities, how they ensured authenticity of records, and if they had even been required to attest to responsibility. These questions can be found in Appendix I.

Seventy-seven percent of respondents said they managed records or information frequently or very frequently, and 67 percent said they conducted retrieval and access, managing or designing metadata (56 percent), and designing information or records policies (51 percent). Monitoring security or access privileges and designing records management systems were the least common activities: 35 percent and 37 percent of respondents respectively reported that they never or infrequently performed these tasks.

When asked to rate social or technological indicators of authenticity according to how frequently they were used to ensure authenticity, more than 50 percent of respondents reported that they relied on traditional (social) archival and records management tools "most of the time" or "always" for managing authenticity, specifically policies governing records (55 percent) and record systems (60 percent), documentation about records systems (51 percent), classification schemes (61 percent) and retention and disposition schedules (51 percent). Fifty-three percent of respondents used access controls and security measures, and 54 percent employed standardized metadata "most of the time" or "always." However, 51 percent of respondents never or rarely relied on audit logs in the course of their work, and 61 percent never or rarely used cryptographic validation techniques.

Of specific cryptographic techniques employed, digital signatures were the least relied upon. Only 11 percent of respondents used digital signature technology

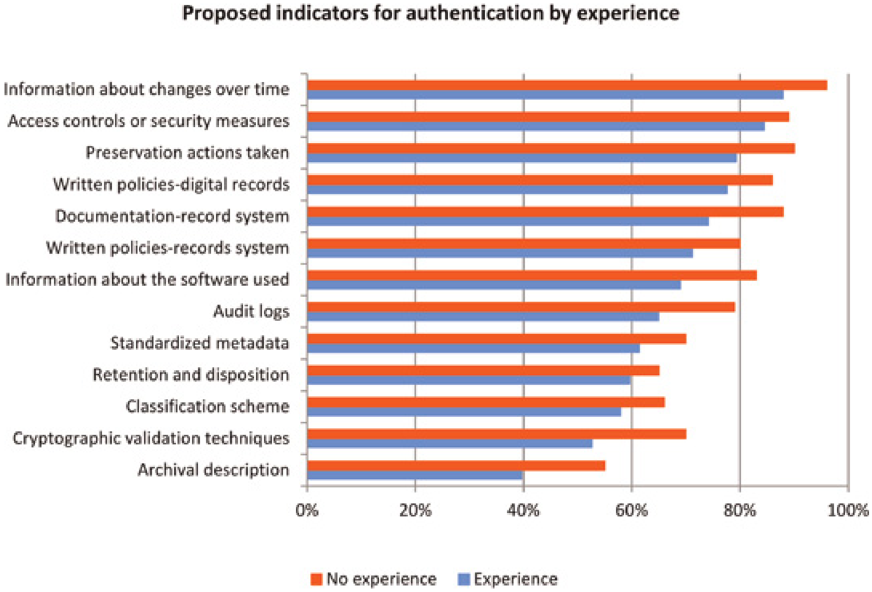

Figure 3: Comparison of indicators of authenticity (n = 247)

to ensure authenticity, and 61 percent never used this technology. Only 5 percent of respondents had been required to attest to authenticity of records in a court proceeding, and 10 percent had been involved in e-discovery or legal hold. Seventy percent of respondents had never been required to attest to the authenticity of records in their care for any purpose, including reference or access.

Respondents who had been required to attest to the authenticity of records or data were asked what indicators they had used in that attestation, while those who had never been required to attest to authenticity were asked what they believed would be necessary in the event that they were so called. The indicators most frequently used by respondents who had been required to attest to authenticity were policies about the digital records in question, information about access controls, and information about changes to the material. Respondents who had not been required to attest to authenticity inflated their belief in the value of all indicators. However, the greatest difference in choice of indicator was found in information about the preservation activities, use of standardized metadata, documented changes to information, information about software, and use of cryptographic techniques (see Figure 3).

When asked to rate their belief in the importance of indicators of authenticity if required to make an attestation of authenticity in a legal or administrative action, 68 percent of respondents said that standardized metadata would be very important or extremely important, cryptographic validation techniques were deemed very or extremely important by 66 percent, audit logs were favoured by 76 percent, and access controls and security measures were considered very or extremely important by 88 percent of respondents. Despite their current practice, therefore, technical means of validating authenticity were considered as important as traditional means. With respect to organizational records and information policies, 54 percent of respondents said their organization did not define authenticity of digital material, and 17 percent did not know if their organizational policies contained such definitions.

Preliminary analysis of the narrative responses to the final two questions (what is your definition of authenticity of digital records and what do you believe is essential to proving the authenticity of digital records?) reveal that authenticity is still generally assessed according to traditional social heuristics. In response to the first question, several respondents noted that records produced in the usual and ordinary course of business could be presumed authentic, thus reflecting statute and precedent law governing business records in common law traditions. Most respondents noted integrity as a means of establishing authenticity, and several stated that bitwise integrity was necessary after the moment a record was "fixed"—that is, chosen to be kept as evidence of the action represented in the record or preserved for long-term reference in an archives. Responses generally indicated a pragmatic approach to authenticity, for example, one respondent answered:

> Is [the record] sufficient for the purposes it may be used for? Would it satisfy a judge or adjudicator? Whatever I can claim about it, can I back that up with facts? / The basic definition of an authentic record is "Can it be used as an authentic record in a situation where an authentic record would be needed?" This is not a yes/no answer (though the question is), but rather a range. I want the records as authentic as they need to be for future uses. They needn't be the MOST authentic—just authentic enough.

The final question explored respondents' beliefs about essential indicators of authenticity. Answers focused on chain of custody, controls on creation and management, policies on access and ensuring provenance information, and the addition or presence of metadata about the creator and context of creation. Several respondents noted the importance of cryptographic validation techniques, and several specifically stated that security and access controls were paramount (although one respondent noted the importance of these controls in the context of using public cloud-based email and document sharing).

This early exploration of the survey data points the way to further research to explore in greater depth the importance of social versus technical indicators of authenticity and how these are used when authenticity is questioned in legal or administrative hearings. Next steps will include further coding and analysis, particularly of the open-ended survey questions, followed by semi-structured interviews with many of those who indicated their willingness to provide more information. The applicability and authority of indicators of authenticity of digital records and data will be assessed in different environments, in particular, when records and data are created, maintained, or preserved in cloud-computing applications. This will be of increasing importance as more organizations turn to cloud service providers to support their operations and as courts continue to face the increasing challenge of evidence presented in digital form.

Limitations

Web-based surveys are convenient ways in which to reach a broad population quickly, but they do have limitations. Primary among these limitations is the inability to be assured of a representative sample. Even when using professional listservs (where the sample members can be reasonably assured of common purpose, training, and responsibility), respondents choose to reply, and while all respondents may be members of the target population, not all members of that population are members of, or have access to or read, these listservs. Generalizability of the results, therefore, is limited, and validity cannot be objectively measured. However, as an indicator of general practice, such surveys provide useful information.

Conclusions

Preliminary findings indicate that records professionals still tend to rely on traditional heuristics for ensuring authenticity, even when they claim to put their trust in more technical solutions if required to attest to authenticity. Records and information professionals—archivists and records managers—have traditionally been the trusted professionals who keep records safe, authentic, and reliable. As complex technology increasingly mediates between the record and the record user, records professionals necessarily place their trust in information technology professionals. It appears that the trusted records professional is now becoming the trusting technology user—the trustee has become the trustor. However, each discipline has unique and complementary knowledge. The records professional knows what information in the form of records and data has value and must be preserved and the information technology professional understands how to protect and secure that information. If our documentary heritage is at the root of democracy and accountability, both professions are necessary in its authentic preservation.

Notes

1. International Data Corporation, http://www.idc.com, is a prominent global provider of intelligence for the information technology, telecommunications and consumer technology markets.
2. *Federal Rules of Evidence*. http://www.law.cornell.edu/rules/fre.

References

ARMA International. 2014. *ARMA Generally Accepted Recordkeeping Principles*. http://www.arma.org/r2/generally-accepted-br-recordkeeping-principles.

Asssociation of Canadian Archivists. 1999. *Code of Ethics: The Association of Canadian Archivists*. http://archivists.ca/content/code-ethics.

Black's Law Dictionary. n.d. 2nd ed. http://thelawdictionary.org/.

Duncan, C. 2009. "Authenticity or Bust." *Archivaria* 68: 97–118.

Duranti, L. 1993. "The Archival Body of Knowledge: Archival Theory, Method, and Practice and Graduate and Continuing Education." *Journal of Education for Library and Information Science* 34 (1): 8–24. http://dx.doi.org/10.2307/40323707.

——. 1997. ''The Archival Bond.'' *Archives and Museum Informatics* 11 (3/4): 213–18. http://dx.doi.org/10.1023/A:1009025127463.

——. 1998. *Diplomatics: New Uses for an Old Science*. Lanham, MD: Scarecrow Press.

——. 2005a. ''The Long-Term Preservation of Accurate and Authentic Digital Data: The InterPARES Project.'' *Data Science Journal* 4: 106–18. http://dx.doi.org/10.2481/dsj.4.106.

——. 2005b. *The Long-Term Preservation of Authentic Electronic Records: Findings of the InterPARES Project*. San Miniato: Archilab.

——. 2009. ''From Digital Diplomatics to Digital Records Forensics.'' *Archivaria* 68 (2): 39–66.

Duranti, L., and B. Endicott-Popovsky. 2010. ''Digital Records Forensics: A New Science and Academic Program for Forensic Readiness.'' *Journal of Digital Forensics, Security and Law* 5 (2): 1–12.

Duranti, L., and H. MacNeil. 1997. ''The Preservation of the Integrity of Electronic Records: An Overview of the UBC-MAS Research Project.'' *Archivaria* 42 (1): 46–67.

Duranti, L., and G. Michetti. 2015. ''The Archival Method: Rediscovering a Research Tradition.'' In *Research in the Archival Multiverse*, ed. Anne Gilliland, Sue McKemmish, and Andrew Lau. Melbourne, Australia: Monash Publishing.

Duranti, L., and R. Preston. 2008. *Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential. Interactive and Dynamic Records*. Padova: Associazione Nazionale Archivistica Italiana.

Duranti, L., and K. Thibodeau. 2006. ''The Concept of Record in Interactive, Experiential and Dynamic Environments: The View of InterPARES.'' *Archival Science* 6 (1): 13–68. http://dx.doi.org/10.1007/s10502-006-9021-7.

Eastwood, T. 1994. ''What Is Archival Theory and Why Is It Important?'' *Archivaria* 37 (1): 122–30.

EMC Corporation. 2013. *Leaders Edge: Highlights from CIO Summit 2013*. Atlanta, GA: EMC Corporation. http://www.emc.com/microsites/cio/articles/cio-summit-2013/cio-summit-2013-atlanta.pdf.

Endicott-Popovsky, B., D.A. Frincke, and C. Taylor. 2007. ''A Theoretical Framework for Organizational Network Forensic Readiness.'' *Journal of Computers* 2 (3): 1–11. http://dx.doi.org/10.4304/jcp.2.3.1-11.

International Organization for Standardization. 2001. *ISO-15489 (2001) Information and Documentation-Records Management*, No. ISO-15489 (2001). http://www.iso.org/iso/catalogue_detail?csnumber=31908

InterPARES Glossary. n.d. *InterPARES 2 Project: Terminology Database*. http://interpares.org/ip2/ip2_terminology_db.cfm.

John, J.L. 2012. *Digital Forensics and Preservation*: Digital Preservation Coalition. http://www.dpconline.org/component/docman/doc_download/810-dpctw12-03pdf.

Kirschenbaum, M.G., R. Ovenden, and G. Redwine. 2010. *Digital Forensics in Born Digital Cultural Heritage Collections*. Washington, DC: Council on Library and Information Resources.

Lauriault, T.P., B.L. Craig, D.R.F. Taylor, and P.L. Pulsifer. 2007. ''Today's Data Are Part of Tomorrow's Research: Archival Issues in the Sciences.'' *Archivaria* 64 (2): 123–80.

MacNeil, H., and A. Gilliland-Swetland. 2005. ''Authenticity Task Force Report.'' In *The Long-term Preservation of Authentic Electronic Records*, ed. L. Duranti, 19–65. San Miniato, Italy: Archilab.

MacNeil, H., and B. Mak. 2007. "Constructions of Authenticity." *Library Trends* 56 (1): 26–52. http://dx.doi.org/10.1353/lib.2007.0054.

Mak, B. 2012. "On the Uses of Authenticity." *Archivaria* 73: 1–17.

Pearce-Moses, R. 2005. *A Glossary of Archival and Records Terminology*. http://www.archivists.org/glossary/.

Richards, L. 2014. *Conversation with the Author*. Washington, DC, 13 August.

Rogers, Corinne. 2011. "Trust Me! I'm a Digital Record: Findings from the Digital Records Forensics Project." Presented at the Archives 360, Society of American Archivists, Chicago, IL, 27 August.

Society of American Archivists. 2011. *SAA Core Values Statement and Code of Ethics*. http://www2.archivists.org/statements/saa-core-values-statement-and-code-of-ethics.

Statistics Canada, Standards Division. 2012. *North American Industry Classification System (NAICS) Canada*. Ottawa, ON: Statistics Canada. http://www.census.gov/eos/www/naics/.

Turner, V., J. Gantz, D. Reinsel, and S. Minton. 2014. *The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things*, White Paper no. IDC 1672. Toronto: IDC Corporation. http://idcdocserv.com/1678.

Appendix A. Survey

How often do you conduct the following tasks with respect to digital records (e.g. electronic documents, images, data, data sets, database records, electronically stored information [ESI], web pages, etc.)? If self-employed or retired, please refer to the job or contract you feel is most relevant. (Never; Rarely; Sometimes; Often; Very Often)

- Conduct retrieval and access
- Monitor or enforce security/access privileges
- Monitor or enforce privacy of personal information
- Monitor or enforce compliance with record keeping regulations/policies (including e-discovery)
- Conduct preservation or curation
- Design systems for storage and management of records
- Design information/records policies
- Manage records or information
- Manage/design metadata
- Other

When you create or manage digital records, how often do you rely on or apply the following to ensure their authenticity? (Never; Rarely; Sometimes; Most of the time; Always)

- Written policies and procedures governing the management of the records system
- Documentation about the record system (design, operation, management, etc.)
- Written policies and procedures governing digital records

- Information about the software used to create and manage the digital records
- Information about changes made to the digital records over time (e.g. migration, normalization, etc.)
- Information about actions taken to preserve the digital records
- Classification scheme and/or file plan
- Retention and disposition schedules
- Archival description
- Access controls/security measures
- Audit logs
- Cryptographic validation techniques (e.g. digital signatures, hash digests, etc.)
- Standardized metadata

How frequently do you use the following cryptographic validation techniques?

- Digital signatures
- Trusted time stamps
- Checksums
- Hash digests
- Secure transmission

What metadata do you routinely use or manage? Please check all that apply.

- A metadata schema or guideline (e.g. Dublin Core, PREMIS, MoReq, etc.) Please list: ____________________
- A modification of a schema, customized for your organization. Please describe: ____________________
- A custom-built metadata schema (designed without elements from existing schemas). Please describe: ____________________
- Metadata generated by the software or record system in use only
- Not sure

Have you ever been required to guarantee or attest to the authenticity of digital records in any of the following circumstances?

- Providing testimony in court or administrative hearing
- Pending litigation or administrative action (e-discovery process)
- Authenticating copies of digital records for research or in response to reference requests
- Other ____________________
- I have never been required to guarantee or attest to the authenticity of digital records

When you were required to guarantee or attest that digital records are authentic, how important were the following in making your assessment? (Not at all important; Very unimportant; Neither important nor unimportant; Very important; Extremely important)

- Written policies and procedures governing the management of the records system

- Documentation about the record system (design, operation, management, etc.)
- Written policies and procedures governing digital records
- Information about the software used to create and manage the digital records
- Information about changes made to the digital records over time, (e.g. migration, normalization, etc.)
- Information about actions taken to preserve the digital records
- Classification scheme and/or file plan
- Retention and disposition schedules
- Archival description
- Access controls/security measures
- Audit logs
- Cryptographic validation techniques (e.g. digital signatures, hash digests, etc.)
- Standardized metadata

If you needed to assess that digital records are authentic, how important would the following be in making your assessment? (Not at all important; Very unimportant; Neither important nor unimportant; Very important; Extremely important)

- Written policies and procedures governing the management of the records system
- Documentation about the record system (design, operation, management, etc.)
- Written policies and procedures governing digital records
- Information about the software used to create and manage the digital records
- Information about changes made to the digital records, (e.g. migration, normalization, etc.)
- Information about actions taken to preserve the digital records
- Classification scheme and/or file plan
- Retention and disposition schedules
- Archival description
- Access controls/security measures
- Audit logs
- Cryptographic validation techniques (e.g. digital signatures, hash digests, etc.)
- Standardized metadata

Based on a consideration of storage only, how much confidence would you have in the authenticity of records in the following storage options, all else being equal? (No confidence; Little confidence; Neither confidence nor lack of confidence; Considerable confidence; Total confidence)

- Digital records stored by their creator on removable media (i.e., a USB key/external hard drive, optical or magnetic media)
- Digital records stored by their creator on stand-alone computers
- Digital records stored by their creator in network drives/filing system
- Digital records in cloud storage maintained by a third party cloud service provider
- Digital records stored by an archives

- Traditional (e.g. paper, microfilm) records stored on- or off-site by their creator
- Traditional records stored by a third party that is not an archives
- Traditional records stored by an archives

Do your organization's records policies define authenticity of digital records?

- Yes
- No
- Don't know

What is your definition of authenticity of digital records?

What do you believe is essential to proving the authenticity of digital record?