Trust and Authenticity in the Digital Environment: An Increasingly Cloudy Issue

Luciana Duranti

"*Whatever* matters to human beings, trust is the atmosphere in which it thrives." (Sissela Bok)

Trust has been defined in many ways, but, at its core, it involves acting without the knowledge needed to act. It consists of substituting the information that one does not have with other information. For example, a person who does not have the knowledge necessary to assess the authenticity of a record relies on the credentials of the expert who authenticates it. Traditionally, trust in records is based on four types of knowledge about its custodian: *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 fulfill his or her current responsibilities as specified by the truster; c*ompetence*, which consists of having the knowledge, skills, talents, and traits required to be able to perform a task to any given standard; and c*onfidence*, which is an assurance of expectation of action and conduct the truster has in the trustee.

In contemporary practice individuals and organizations are increasingly saving and accessing records in the highly networked, easily hacked environment of the Internet, where current policies, practices and infrastructure prohibit us from being able to assess our trust in records using the four types of knowledge used in the past. People trust banks, phone companies, hospitals, government, etc. to keep and maintain their digital data/records/archives on their behalf. However, where their records actually reside, how well they are being managed, how long they will be available to them... they have no idea! Many organizations are becoming concerned about a liability they may not have thought they were assuming. Others are amassing huge volumes of data that they use to provide a host of services, many of which focus on marketing and securing competitive advantage. This is the world of the so-called 'big data', the exploitation of seemingly innocuous records (e.g. purchase orders) to produce data that can be re-manipulated to serve a host of purposes, not always noble. However, big data also fosters a range of democratic objectives, from promoting government transparency to supporting research to contributing to public-private sector goals and priorities.

The issues presented by this scenario are clear: Can the data be trusted? Can the records from which the data are derived be trusted or even traceable? Are they complete? Are they authentic? How were they generated and by whom? How are they stored and under what jurisdiction? Who has access to them? How secure are they? Organizations realize that their data and records holdings are digital assets that need to be managed effectively if they are to be trusted by those making decisions and by clients, customers, citizens, etc.

This presentation will identify the salient differences between digital and traditional records as forms of writing, and will discuss the issues related to the authentic preservation of digital records over the long term. In the digital environment authenticity is an inference based on foundation evidence. To presume it through a contextual assessment, verify it through comparison or demonstration, or declare it through authentication requires trust in the reputation, performance, and competence of the keeper or preserver of the digital entities at issue. However, it also requires transparency and accountability, supported by a strong legal framework. Such framework can be based on the principles of diplomatics and archival science, as recommended by two international research projects, the Digital Records Forensics (DRF) Project and the International research on Permanent Authentic Records in Electronic Systems (InterPARES) Project, whose conceptual findings will be outlined.

The presentation will discuss the concept of authenticity in relation to those reliability, accuracy and authentication and analyse its components, identity and integrity, in a digital context, especially with regard to bit-streams, data, duplicates, technological environment (computer and system), and processes. The presentation will be concluded by a demonstration of how the concepts outlined can be used to assess the viability or lack thereof of a cloud environment for recordkeeping and preservation, focusing on its viability, trustworthiness, legal risks, operational risks, and costs-benefits.