Trust and Conflicting Rights in the Digital Environment

Dr. Luciana Duranti
The University of British Columbia, School of Library, Archival and Information Studies

Abstract
While evolving and emerging digital technologies serve the needs of governments, businesses and individuals to great advantage, the often unintended consequences of their use may be harmful. When WikiLeaks began publishing the largest set of confidential documents ever released, it exposed how endangered are our cherished, yet sometimes conflicting rights--secrecy vs. transparency, privacy vs. access--in the digital world. Moreover, making, storing and accessing records in the highly networked, easily hacked environment of the Internet, is creating liabilities that institutions may not have thought they were assuming. Can the data be trusted? Can the documents from which the data are derived be trusted or even traceable? Are they complete? Are they authentic? Who has access to them? How secure are they? The overview of these and other legal challenges provides a framework for the presentations discussing them.

Author
Luciana Duranti is Chair of Archival Studies at the University of British Columbia, and a Professor of archival theory, diplomatics, and the management of digital records in its master's and doctoral archival programs. She is Director of the Centre for the International Study of Contemporary Records and Archives (CISCRA) and, among many research projects about the issues presented by digital records, InterPARES, Digital Records Forensics, and Records in the Clouds. She is co-Director of "The Law of Evidence in the Digital Environment" Project. Duranti is active nationally and internationally in archival associations and committees, such as the UNESCO International Advisory Committee of the Memory of the World Program; and has been the President of the Society of American Archivists, of which she is a Fellow. She publishes widely on archival theory and diplomatics.

"*Whatever* matters to human beings, trust is the atmosphere in which it thrives" Sissela Bok[1]

On November 28, 2010 WikiLeaks began publishing the largest set of confidential documents ever released, provoking the outrage of governments worldwide, regardless of the many individual voices claiming the morality of such action. Revelation of secret documents is nothing new. What is new is the scale of the phenomenon. Technology has allowed for the uncontrolled growth of databases that can be accessible from any distance. With the amount of data/documents/records created and maintained in digital form, there is a new social awareness of their information potential, and the ease with which they

[1] Sissela, B. (1978). *Lying*. New York: Pantheon Books.

can be disseminated highlights the vulnerability of all parties involved. This fact in itself is at the root of a redistribution of power – the right to know is becoming the core of a new form of democracy that refuses to be held captive to old mechanisms. The WikiLeaks model is destined to spread. TradeLeaks and BrusselLeaks are examples, claiming to reveal frauds in commerce and in the political dealings of European Union members, but in the process, risking damage to the rights of individuals, organizations and governments, as well as to their legitimate operations. These developments are resulting in demands for increased security surrounding digital information, but technology is not the whole answer. *The challenge is providing transparency while protecting the arcana imperii (state secrets).*

In an interesting twist, WikiLeaks entrusted the selection and dissemination of the information to five newspapers for the purpose of avoiding making available data that would hurt military operations or human beings. The old press put its authority at the service of rights to transparency and access by helping certify the reliability and authenticity of the documents, a function of vital importance when their origin is not known and the accuracy of their content may be in doubt. *The challenge is establishing documents' accuracy, reliability and authenticity and maintaining it over time in such a way that it can be proven.*

It is worth noting that Sweden, which in 1766 passed the oldest freedom of information law, is the country that most fiercely condemned the WikiLeaks disclosure. But condemning an action does not prevent its repetition. Iceland recently approved a law that allows for the publication of secret documents. Germany is following suit and so are other countries. Developing new legislation for access requires a profound understanding of the digital environment, of the information generated within it and the various forms it takes, and the way it relates to actions, transactions and facts. *The challenge is to develop legislation and procedures based on an understanding of the way in which digital records serve and protect the rights of the people and of those who govern them.*

In 2009, the Information Commissioner of Canada, in a report entitled *A Dire Diagnosis for Access to Information in Canada*, wrote: "The poor performance shown by institutions is symptomatic of what has become a **major information management crisis** (emphasis original). A crisis that is only exacerbated with the pace of technological developments. Access to information has become hostage to this crisis and is about to become its victim. There is currently no universal and horizontal approach to managing or accessing information within government. Some institutions don't even know exactly what information they are holding."[2] *The challenge is to develop an infrastructure that ensures a seamless controlled flow of authentic data/documents/records from the creator to the preserver irrespective of changes in technology.*

The right of societies to an enduring documentary heritage became the mission in 1992 of the UNESCO Memory of the World Program. The program inscribes in its registers the records of human achievements as well as those of the darkest moments of human history. It is now grappling with the development of guidelines for the preservation of nominated digital material, which will enable custodians to ensure its continuing authenticity and reliable permanent preservation. *The challenge is to provide guidance to countries, organizations and individuals with different resources and from different cultures, connected by the Internet but divided by their ability to realize its potential while protecting themselves from its risks.*

[2] Office of the Information Commissioner of Canada. (2009). *A Dire Diagnosis for Access to Information in Canada.* Online: http://www.oic-ci.gc.ca/eng/med-roo-sal-med_spe-dis_2009_4.aspx.

The challenges described show that several conflicting rights, directly linked to the creation, management and preservation of data, records and archives, are at risk in the digital environment**: the right to transparency and to secrecy, the right to access and to privacy, the right to knowledge and to economic gain, the right to dissemination of one's work and to its integrity, the right to memory and to right to be forgotten, the right to the endurance of one's heritage and the right to oblivion.** How can we protect these conflicting rights? Whom and what can we trust with the care of the digital objects that embody them, attest to them, support them, result from them, are the object of their exercise, or disseminate them so that they can be nurtured, respected, guaranteed, and regarded as certain and clear? The certainty of people's rights as objectified in the world' documentary residue is one of the pillars of every democratic society**.** As Baldassare Bonifacio wrote in 1630:

> There is nothing more necessary for clearing up and illustrating obscure matters...for conserving patrimonies and thrones, all things public and private, than a well constituted store of volumes and documents and records--as much better than navy yards, as much more efficacious than munition factories, as it is finer to win by reason rather than by violence, by right than by wrong.[3]

And as Sir Hilary Jenkinson re-stated three centuries later, documents are "the material evidence of the historical case."[4] Again, whom or what do we entrust with this invaluable store of rights?

Traditionally, trust in documents has been based on trust in those who hold them in custody. The grounds for it are: *reputation*, which results from an evaluation of the custodians' past actions and conduct; *performance*, which is the relationship between the custodian's present actions and the conduct required to fulfil his or her current responsibilities; 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.[5] With respect to the digital material produced by contemporary society in both the public and private sphere, do we still have confidence in the competence, performance and reputation of those who have it in their custody? If we do, should we? Is the legal framework in which they operate strong enough to ensure that our trust is well placed?

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 relying on the kind of understanding we used in the past. How do we know that those who hold digital records about us make the right decisions about keeping them safe, and accessible only to those who have a right to see them, using them for good and in a transparent way, disposing of them when required, and selecting reliable Internet providers for storing and managing them? Who has established the rules according to which they operate, and in the context of what values and purpose?

The interconnectedness of the Internet is forcing us into one community without the benefit of gradually getting to know one another. As the United States developed the Internet, its social, political,

---

[3] Born, L. (1941). "Baldassarre Bonifacio and His Essay *De Archivis*," *The American Archivist* IV, 4: 233-234.
[4] Jenkinson, H. (1980). "The English Archivist: A New Profession," in *The Selected Writings of Sir Hilary Jenkinson* (Gloucester), pp. 246–47.
[5] Borland, J. (2009). "Trusting archivists." *Archivi & Computer*, XIX(1):96–109; Duranti, L. and Rogers, C. (2011). "Educating for Trust," *Archival Science,* Volume 11, Issue 3, pp. 373-390. Online: SpringerLink DOI: 10.1007/s10502-011-9152-3. See http://www.springerlink.com/openurl.asp?genre=article&id=doi:10.1007/s10502-011-9152-3; Sztompka, P. (1999). *Trust*. Cambridge University Press, Cambridge.

and economic views are reflected in its management, thereby rankling other countries. A recent example highlights the risks of using a consumer file-sharing service for business purposes when it is not clear what legal framework controls it. U.S. federal prosecutors blocked access to the file-sharing site Megaupload.com on charges that the site violated piracy laws, and New Zealand police arrested Megaupload's founder based on the U.S. accusations. As a consequence the data of at least 50 million Megaupload users ran the risk of being erased.[6] Convinced that existing laws could not deal with growing piracy concerns, the U.S. Congress introduced the *Stop Online Piracy Act (SOPA*), which resulted in protests across the Internet that persuaded Congress to reject the bill. In the meanwhile, the European Union proposed a "right to be forgotten" directive, which would have required every member state to issue legislation protecting online intellectual rights and privacy.[7] Thankfully, this initiative also, was unsuccessful, but it shows how unclear is what is best to do. Google established a blanket privacy policy for all materials on its cloud,[8] while Twitter chose to go the opposite way and to adopt the policy of the country of origin of the record.[9] Indeed, the Internet has forced us into one community, but one community in desperate need of a shared legal framework that promotes consistency and balance in terms of policies and practices regarding the handling of digital objects, especially when they reside with Internet services and social media providers.

In fact, regardless of several public cases of dramatic documentary incidents, people in general trust all kinds of organizations, like banks and phone companies, to keep and maintain their data/records/archives on their behalf. In effect they have shifted their trust from the central records repository in their home or office to distributed archives online, the stewardship for which is entrusted to others. 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 recognizing this shift and becoming concerned about a liability they may not have thought they were assuming, especially as more and more clients abandon their own recordkeeping, and place greater reliance and trust on the recordkeeping abilities of the organizations with which they interact.

In additions, commercial organizations like telecommunications services, distributors, and the like, 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 evolving world of big data', the exploitation of seemingly innocuous records, like call centre records, purchase orders, etc., to produce data that can be re-manipulated to serve a host of purposes, also called 'data mining.' Big data is introducing a view of our documentary output that flips our traditional view on its head: certain records can grow in value if it is recognized that their accumulation through time will enable the production of data that themselves will grow in value as their potential to support organizational priorities—especially strategic priorities—is realized. 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. Thus, legislation, regulations, policies are needed to control these activities so that their benefits can be ripped and their risks contained.

---

[6] Maes, J. (2012). "SOPA, PIPA, Megaupload.com, and the United States Government," Washington Times (3 February). Online: http://communities.washingtontimes.com/neighborhood/political-potpourri/2012/feb/3/sopa-pipa-megauploadcom-and-united-states-governme/

[7] http://www.bbc.co.uk/news/technology-16677370

[8] Google (2012). *Preview. Privacy Policy 1 March 2012.* Online: http://www.google.com/intl/en/policies/privacy/preview/

[9] Twitter Blog (2012). "Tweets Still Must Flow." Online: http://blog.twitter.com/2012/01/tweets-still-must-flow.html.

The issues for data and records coincide. Can the data be trusted? Can the records from which the data are derived be trusted? Are they complete? Are they authentic? How were they generated, by whom and under what conditions? Is there sufficient contextual information to enable them to be understood? These are questions faced by quite a number of organizations that are beginning to act on the realization that their data holdings, and the records generating that data, 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. One of the catch words in this arena is 'traceability', that is, the ability of an organization to trace back from the data it is using for decision-making, service delivery, etc. to the source records from which the data are derived. The issue of traceability of data to trusted records is becoming huge and constitutes the foundation of trust in data.

Different but equally significant issues are generated by the fact that individuals and organizations, large and small, are drawn increasingly by the lure of *cloud computing* for the many benefits it offers. Scalable, agile, efficient, on-demand computing resources mean that email, photos, documents, records, and archival fonds can be easily stored and shared through a seemingly endless number of hosted web applications, and that sophisticated software, platforms, and infrastructure are available to the budget-conscious and the technology-resource limited. Cloud architectures offer on-demand access to services across a network of standard internet-accessible devices – mobile phones, tablets, laptops – and a vast array of other equipment, such as game consoles, MP3 players, and e-business technologies. Resources are shared among users, and resource use is monitored and invoiced based on usage for service. We choose – and increasingly rely on – cloud services for communication, backup and storage, collaboration, distribution, recordkeeping and preservation. But for every benefit there is a corresponding risk that may or may not be recognized.

The model of cloud computing is reminiscent of the mainframe environment of the 1960s, except that in this case we are not putting our trust in the proprietary and highly controlled environment of the company mainframe, but in global service providers, whose agendas and priorities as they build out their infrastructures are very different from our own. The trust relationship demands careful analysis and consideration and it is important to highlight specific challenges to entrusting data, records and archives to the cloud. Key issues of ownership, jurisdiction, and privacy have yet to be resolved. Longer term concerns around responsibility for maintenance, access, and preservation, all of which correspond to issues of trust, are looming on the horizon. The following list identifies some legal concerns but is by no means exhaustive:

- The servers in which data and records are stored may be, but likely are not, in the same country or jurisdiction in which they were created. In the event of litigation or other dispute**,** in what jurisdiction will they be governed?
- Do you even know with which provider your material is stored? As the cloud storage market continues to grow, this becomes increasingly unclear. New storage providers are appearing who aggregate unused storage from third parties. The entrance of a peer-to-peer model for storage adds further complexity to teasing out the tangled web of provenance, custody, control, and legal responsibility.
- Will trade secrets or legal privilege, if entrusted to cloud storage, continue to exist after they have been shared with a third party?
- How will cloud service providers protect content from data breaches**?** There is a school of thought that says you should be concerned not about *if* a data breach occurs, but *when* it occurs.

How will your cloud service provider handle a breach? Will your provider even admit to a breach?

- Audit is usually not allowed by cloud providers: How do you prove authenticity and an unbroken chain of custody?
- What happens to content if a cloud service provider goes offline, due to bankruptcy or criminal investigation, or if the server containing your material is sequestered for an investigation?
- How do you transfer the material to the designated cultural institution with independent evidence of chain of custody?

With these questions in mind, returning to the concept of trust and the protection of rights embodied in and exercised through data, documents, records, archives, if trust rests on our confidence in the reputation, performance, competence, and confidence of the custodian of our digital material, we must ask hard questions of those to whom we entrust our data, records and archives. International research projects into the nature of digital records have developed guidelines and solutions to managing authenticity, accuracy and reliability in digital records systems, but solutions are often out of reach financially for many individuals, organizations and countries driven by the bottom line. National and international standards of records and information management provide guidance but adherence is not legally required in most sectors. Cloud computing offers to ease the financial burden of many aspects of records management and archival storage, but—as we have seen—raises a host of new and troubling questions that must be answered if we are to be able to trust and maintain access to our material. Technology will not stand still to wait for our legal and regulatory system to catch up. Even if it did, domestic legislation, as controlled as it is by the higher law of each country, and, in common law countries, also by case law, would often be conflicting with that of other jurisdictions, and, looking at the world map, we would be seeing a tower of Babel of legislations that create more problems than they can solve.

What we need is an internationally agreed upon legal framework that will support the development of integrated and consistent local, national and international networks of policies, procedures, regulations, standards and legislation concerning digital records, to ensure public trust grounded on evidence of good governance. Such legal framework needs to anticipate problems in maintaining any trust in digital data/records/archives which are now under the control of entities suffering a waning level of confidence from the public, including legal, law enforcement, financial, medical, broadcasting, and governmental organizations and professionals, especially in light of the noted exponential growth of and reliance on Internet services. This could be done by means of "model legislation" that can be adapted to each national and cultural context. This model legislation would allow for a harmonization of provisions related to the proper control of our digital heritage from the moment of creation throughout its life-cycle so that it will be produced and maintained in an accurate and reliable way and its authenticity will be protected from the very beginning. A model legislation needs to be detailed enough to contain exemplary norms about specific issues presented by digital material, but general enough to be independent of technological changes, focusing on concepts rather than processes, principles rather than activities.

The only body which can take up the responsibility of writing this non-legally binding model law for the protection of the rights embodied in and exercised through digital documents, and which has the authority and the recognition for doing so is UNESCO. UNESCO can issue a model law as a recommendation, that is, as an instrument in which "the General Conference formulates principles and

norms for the international regulation of any particular question, and which invites Member States to take whatever legislative or other steps may be required in conformity with the constitutional practice of each State and the nature of the question under consideration to apply the principles and norms aforesaid within their respective territories" (Article 1 (b))." The UNESCO Charter on the Preservation of Digital Heritage, whose purpose is to guide the member states in overcoming the challenges of digital preservation, as revised on the basis of the recommendations coming out of this conference, is the ideal contextual document for a model law. As its natural complement, a model law would guide the legislative bodies of the member states in ensuring the proper implementation of the Charter's general guidance through the issuing of domestic legislation. This conference is the time to start thinking what a model law should include. If not now, when?