



**Digitizing the World's Laws:
Authentication and Preservation**

Claire M. Germain
Cornell Law Library
Ithaca, NY/USA
E-mail: cmg13@cornell.edu

Meeting: **96. Law Libraries, Government Libraries and Government
Information and Official Publications**

WORLD LIBRARY AND INFORMATION CONGRESS: 76TH IFLA GENERAL CONFERENCE AND ASSEMBLY
10-15 August 2010, Gothenburg, Sweden
<http://www.ifla.org/en/ifla76>

Abstract:

Many countries now provide online access to statutes, codes, regulations, court decisions, and international agreements. Digital law issues that have emerged include authentication of official legal information and preservation for long term access, particularly for born digital legal information which has no paper equivalent. This article is part of a chapter forthcoming in "International Legal Information Management Handbook" (Ashgate 2010).

A World Snapshot

Many countries now provide online access to statutes, codes, regulations, court decisions, and international agreements. The focus here is on official legal information coming from governments world-wide. To assess progress, in early 2010 I conducted an empirical survey of as many as possible of the 192 countries listed by the United Nations, mostly by going directly to the government websites of each country. Two online guides were particularly useful: the New York University Globalex research guide series (free, <<http://www.nyulawglobal.org/globalex>>) and Reynolds and Flores's *Foreign Law Guide* (fee-based, <www.foreignlawguide.com>) are both thorough and thoughtful, well researched, and provide context for the primary and secondary sources (in common law terminology), as well as a standard table of contents for each country, which is useful for comparisons. This first world snapshot shows much progress and the overall picture that emerges is very positive, showing world-wide evolution toward the availability of more information.¹ However, because the digital medium is vulnerable to errors and

¹ For more information on the study, see a preliminary version at
http://scholarship.law.cornell.edu/clsops_papers/72/.

tampering, it is of utmost importance to make digital legal information official and authentic. In addition, there are special concerns for the preservation of long term access to born digital content with no paper equivalent.

Official and Authentic Digital Legal Sources

The terms “official” and “authentic” are sometimes used interchangeably but mean different things. An online official legal resource is one that possesses the same status as a print official legal resource. In the United States, for instance, the definition of an official version of court opinions, statutes, session laws, or regulatory materials is one “that has been governmentally mandated or approved by statute or rule. It might be produced by the government, but does not have to be.” (American Association of Law Libraries 2007) This definition is firmly rooted in the print world. Courts and public officials turn to official legal resources for authoritative and reliable statements of the law and require citation to such sources in the documents that come before them. By itself, an online official legal resource offers no such automatic assurance.

Authenticity refers to the quality and credibility of the document. It means that the text is provided by competent authority and that it has not undergone any alteration in the chain of custody.² An online authentic legal resource is one for which a government entity has verified the content to be complete and unaltered from the version approved or published by the content originator. Typically an authentic text will bear a certificate or mark certifying that the text is authenticated. The standard methods of authentication include encryption, especially digital signatures and public key infrastructure (PKI), or similar technologies.³ Authentication of digital law varies by country; some provide authentication through a digital signature or PKI infrastructure, others through secure servers and certificates (Hietanen 2007).

Some countries do not recognize the official status of their electronic publications. Bermuda, for instance, states on its web site that “[T]he laws on this website are provided for informational purposes only and do not yet have official sanction (<<http://www.bermudalaws.bm/disclaimer.html>>, accessed 21 June 2010). The European Union Eur-Lex Website states that “Only European Union legislation published in paper editions of the Official Journal of the European Union is deemed

² The International Organization for Standardization (ISO) has published standard ISO 15489-1 Information and Documentation—Records Management. Clause 7.2.2. defines authenticity: “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” (Aki 2007, 9).

³ A Public Key Infrastructure (PKI) is “an asymmetric cryptography security environment that supports the transmission, delivery, and receipt of digital communications over a non-secure communications channel. PKI uses a pair of cryptographically related keys known as public and private keys which verify the identity of the sender (signing) and/or ensure privacy (encryption).” Information provided by Mike Wash, Chief Technical Officer, US Government Printing Office.

authentic.” (<http://eur-lex.europa.eu/en/editorial/legal_notice.htm>), accessed 21 June 2010). Other countries declare their digital law documents to be official and authentic. In France, the *Journal Officiel* electronic version has been declared authentic (authenticated) since 2004. (<<http://www.journal-officiel.gouv.fr/>>, accessed 21 June 2010) In Brazil, until December 2002, the texts of legal rules available on the Internet had only an informative nature. With the advent of Decree No. 4,520, all official documents are published by the Official Gazette of the Federal Government and the Official Gazette of the Justice, are available at the official web site of the National Press, and are certified by the Brazilian Public Key Infrastructure (ICP-Brazil), thus giving them the same authenticity and validity as the printed ones. Canada states that its consolidated legislative texts have official status and are admissible in court. (<<http://laws-lois.justice.gc.ca/eng/FAQ>>, accessed 21 June 2010).

Authenticity matters because in an environment where online sources are replacing official print versions of legal information, citizens need to be able to trust digital versions of the law, in the same way that they have trusted print. Because the digital medium is vulnerable to errors in management and control, corruption, and tampering, it is of utmost importance to make digital legal information not only official but authentic. What is at stake is the transmission of official documents, "the word of the law," to future generations (Germain 1999).

In the United States, the American Association of Law Libraries (AALL) has been active and successful in encouraging federal and state government entities to take the necessary steps to ensure authentic digital law. As AALL President in 2006, I commissioned an AALL Fifty State Survey, which revealed that a significant number of the state online legal resources were deemed official, but none were authenticated by standard methods. (American Association of Law Libraries 2007)⁴ A subsequent National Summit on Authentic Legal Information in the Digital Age in 2007 (<<http://www.aallnet.org/summit/>>, accessed 21 June 2010) prompted the US National Conference of Commissioners on Uniform State Laws (NCCUSL) to investigate online authentication of legal materials. In January 2010, NCCUSL issued a draft Authentication and Preservation of State Electronic Legal Materials Act to assist states in preparing legislation on authenticating and preserving electronic legal materials, which was considered at its July 2010 annual meeting.

At the federal level, the US Government Printing Office (GPO) Federal Digital System (FDsys) provides information from all three branches of government (executive, legislative, and judicial) and keeps it permanently available in electronic format, authenticated, with version control, and accessible via the web for searching, viewing, downloading, and printing (<<http://www.gpo.gov/fdsys/>>, accessed 21 June 2010).

European countries use a variety of measures to ensure authenticity, but some countries do not take special measures. Estonia uses secure servers (<<https://www.riigiteataja.ee/ert/intr/en.htm>>, accessed 21 June 2010). The Canadian province of Ontario does not specify any special authentication of their documents:

⁴ The survey investigated six sources of law: state statutes and session laws, state high and intermediate appellate court opinions, and state administrative codes and registers. For each, the question asked was: is the digital version considered official? Is it considered authentic?

A copy of an official law that is printed by the Queen's Printer or accessed from the e-Laws website in a prescribed form or format is an official copy of the law, unless there is a disclaimer indicating that it is not official. Unless the contrary is proved, official copies of the law are accurate statements of the law " (Ontario 2006).

GLIN's security policy assures users that the full text is a true representation of the source material, has not been modified, and is a certified document from GLIN. For new texts the Certification of Authenticity is issued by an authenticated user and carries a signature (<http://www.glin.gov/helpTopic.action?topic=9010>>, accessed 21 June 2010).

The importance of authentication of digital law is perceived differently in different countries. Some are still exploring the challenges of putting laws online; their first priority is the quality of texts and their accessibility (Petitcollot 2008). Overall, it is a goal for countries toward which all countries should strive.

Digital Preservation and Long Term Access

A major problem with digital information is its vulnerability. Under good conditions, official court reports, session laws, and codes printed on acid-free paper will last for centuries. The same information published in digital form may become obsolete within a few years if it is not migrated to a new platform. The technical problems related to the fragility of the digital medium are numerous, as are the legal and policy issues such as who is responsible for preserving the content (Rieger 2008). There are special concerns for the preservation and long term access to born digital content with no paper equivalent. As of 2010, no permanent solutions exist. The best technological systems can only guarantee a fixed number of years, no more than 50 years,⁵ and information needs to be regularly migrated to new software, or to a new platform, so it is not lost.

With legal materials an issue of particular importance is the need to make sure that in a paperless world there will be a permanent record of the law in its many forms, and that the record will be authentic. This is an area where there is a great role for libraries to preserve the digital heritage of mankind (Germain 2006). It is important for libraries to work as partners with governments, the legal information publishing industry, the information technology industry, computer scientists, and other interested stakeholders. Although the field of digital preservation is in a constant state of flux, much progress has occurred over the past decade. A number of interesting projects and organizations have emerged, together with new tools, services and best practices for the preservation of digital content (Rhodes 2010). The issues relate to what intellectual content to preserve, in what systems and formats, and what standards to use. The Open Archival Information System (OAIS) reference model addresses a full range of preservation functions, including ingest, archival storage, data management, access, and dissemination. Specifically applicable to organizations with long-term preservation responsibilities, it has provided a framework and a common language for digital preservation discussions

⁵ Conversation with Ladislav Borhy, SUN Microsystems Czech Republic, at

2009 Caslin meeting in Tepla, Czech Republic, June 2009.

and planning activities, especially for their technical and architectural aspects (Consultative Committee 2002).⁶ An OCLC (Online Computer Library Center /RLG (Research Libraries Group) and National Archives and Records Administration (NARA) task force has developed an Audit Checklist for Certifying Digital Repositories to assess reliability, commitment, and readiness to assume long-term preservation responsibilities (Center for Research Libraries 2007). Another issue is whether to maintain both an open access online repository and a separate dark digital preservation system (Rhodes 2010).

The most prominent archival systems today are HathiTrust, (<www.hathitrust.org> accessed 21 June 2010), LOCKSS (<<http://lockss.stanford.edu/lockss/Home>>, accessed 21 June 2010), and Portico (<www.portico.org>, accessed 21 June 2010). There is no single solution. The following guidelines from Portico, an archiving service, help explain the principles of digital preservation. Although Portico is mainly meant to preserve the content of scholarly journals, the principles can be extended to the preservation of legal information.

The integrity of the scholarly record must be preserved. The archive must accept the content as it was published and should not correct or alter the record.

The archive must preserve the intellectual content of the electronic journal as completely as possible, although we recognize that some electronic content may have already been lost. [...] Portico's primary preservation methodology is migration, which involves transitioning content from one file format to another as technology changes and as file formats become obsolete. An initial migration is performed when the source files are received and normalized to the archival format.

Portico's archival format is based on the open standard Journal Archiving and Interchange DTD and it uses the Metadata Encoding and Transmission Standards (METS) and the Open Archival Information System (OAIS) Reference Model

Among recent noteworthy efforts, the Library of Congress's National Digital Information Infrastructure and Preservation Program (NDIIPP) has funded several projects to preserve state government digital information and implement a trustworthy information management system, to capture, preserve and provide access to "at-risk" digital content from state legislatures (<http://www.digitalpreservation.gov/>>, accessed 21 June 2010). The Chesapeake Project involving three partners, preserves online publications of the Virginia Supreme Court and other entities in the Virginia judicial branch (Dockendorf 2009). The Legal Information and Preservation Alliance (LIPA), founded in 2003 has the mission to preserve vital legal information by defining objectives, endorsing and promoting the use of appropriate standards and models, creating networks, and fostering financial and political support for long term stability (<<http://www.aallnet.org/committee/lipa/>>, accessed 21 June 2010).

Several organizations can host digital content at a secure off site location and manage system updates and migration. Non-profit organizations such as Portico and LOCKSS (Lots of Copies Keep Stuff Safe) function as preservation systems. The Internet Archive offers an "Archive-It" service for the preservation of web sites (<<http://archive-it.org/>>, accessed 21 June 2010). The US Department of Labor contracted with the Internet Archive to take a digital 'snapshot' and archive the content of all departmental Web sites (United States Department of Labor 2009).

The US Library of Congress National Digital Information Infrastructure and Preservation is collaborating with DuraSpace on a pilot program, to test the use of cloud technologies to enable perpetual access to digital content (<http://www.digitalpreservation.gov/partners/duracloud/duracloud.html>), accessed 21 June 2010).

LOCKSS, based at Stanford University Libraries, provides libraries with digital preservation tools and support so that they can easily and inexpensively collect and preserve their own copies of authorized e-content. The technology provides an open source, peer-to-peer, decentralized digital preservation infrastructure, for all formats and genres of web-published content. The intellectual content, which includes the historical context (the look and feel of the texts), is preserved. LOCKSS is OAIS-compliant; the software migrates content forward in time; and the bits and bytes are continually audited and repaired. CLOCKSS (*Controlled LOCKSS*) (<http://www.clockss.org/clockss/Home>), accessed 21 June 2010) is a non-profit joint venture between the world's leading scholarly publishers and research libraries. Its mission is to build a sustainable, geographically distributed dark archive to ensure the long-term survival of Web-based scholarly publications for the benefit of the global research community.

Conclusion

As legal information systems mature worldwide, authenticity is seen as an essential issue by some who want to guarantee the integrity of official information. There is a great role for librarians as the research experts in providing access to legal information and as custodians of information for the long term, in any format, print or digital. The successful advocacy efforts of the American Association of Law Libraries in the USA show that librarians can influence information policy decisions for the benefit of all citizens. There is a great interest in bringing this advocacy to the international level to develop international standards, possibly within the International Federation of Library Associations, a major stakeholder for information policy.