**Background on UELMA**

The Uniform Law Commission (ULC) adopted the Uniform Electronic Legal Material Act (*the* UELMA) at its July 2011 annual conference to provide a uniform Act that helps govern the trustworthiness and authenticity of the information posted on state managed Internet law sites. The ULC developed the UELMA to assure that all state Internet sites that contain legal material conform to uniform standards, as increasing numbers of states are abandoning printed law books for online-only publishing.

The posted legal material--whose categories may be chosen and defined by each state, but at minimum are intended to cover statute and case law books--must be current and authentic, archived, accessible, posted indefinitely, and have all electronic posted versions of laws available, no matter how many times the versions change. The UELMA assumes states will adhere to the law correctly, and that states will create internal standards and practices to ensure that the goals of the statute are fulfilled. But if a state should fail to do so, UELMA nonetheless shifts the burden to disprove the validity of information to the opposing party.

Inevitably, shifting from a print mode to an Internet-based digital mode assumes some risks that are not generally present in print, such as risk of hacking, use of outdated material, broken links and incomplete archives. The digital world has developed some tools to minimize risk, but these are often costly and difficult to use. Regardless, UELMA does not create uniformity for use of these tools, rendering the statute inadequate to achieve its stated goals.

The Public Notice Resource Center (*the* PNRC) continues to express concerns, even after submitting a comment letter collectively with the American Court & Commercial Newspapers (ACCN) and National Newspaper Association to the ULC on February 22, 2011 outlining the UELMA’s flaws. Although the ULC did address a couple of the issues raised, PNRC continues to believe the UELMA still has severe flaws.

For example:

• UELMA is silent on which tools and practices states must use to authenticate electronically posted legal material. Currently, states can select digital watermarking or digital stamping, or other means. Or, hypothetically, a state could take no steps and simply declare its own information trustworthy. Even recognized authentication methods are not without risks from forgeries.

• UELMA requires any state that adopts the UELMA to presume another adoptive state’s legal material is accurate. State judges, the bar and the public would be required by state law to adopt these presumptions, whether or not they have any adequate means to investigate whether they are true. If states are inconsistent in methods of authentication, confusion about the legitimacy of other state’s documents may pose a distraction in legal proceedings.

• UELMA unfairly places the burden to disprove the accuracy of electronic legal material published by states on parties challenging such material. It requires a litigant or a citizen to prove a negative. In other words, readers may be unaware they are not finding an authentic version of a document.

• UELMA does not encourage continuation of printed versions as a way of mitigating risk from the digital versions. It does not specify a preservation method. Today, most digitized legal information is backed with a printed copy somewhere that can be checked against the online version. Without a backup print copy, that safety net is gone. As various versions of laws change over time—either by legislative changes or judicial rulings—the base line and history may be lost forever if web sites do not accomplish adequate archiving.

* UELMA does not, and in fact cannot, ensure that public funding of its mandates will occur over time. If funding fails, and it almost inevitably will at some point in history, electronic copies and archives may be lost forever. At least in a print environment, a dusty tome in a library can usually be resurrected to track the development of a law or policy.

• UELMA does not contain a set schedule that a state must follow to post updates to public Internet sites. It is left to states to decide how or whether to notify the public on the dates of postings, so a reader might be led to suspect that changes in statutes or regulations have superseded the online version.

• Much in UELMA assumes states will use common sense approaches to developing web sites, funding them, providing authentication and archiving. It is an "ends-tested" statute but it provides no means for the public to investigate whether the ends are adequately achieved. Assuming that web sites involving law books will be managed by the courts that are not subject to public records laws, UELMA provides no path for citizens to investigate compliance with UELMA's goals. Similarly, if web sites for statutes are maintained by revisors of the statutes or legislative clerk offices in the states, public records laws generally do not reach these offices, so citizens would likewise not be able to investigate compliance. And there is nothing within the UELMA that would require the state to monitor and report its implementation, success, or failure to the public.

**I. Authentication Problems**

 **Section 6. Effect of Authentication**

 *(a) Legal material in an electronic record that is authenticated under Section 5 is presumed to be an accurate copy of the legal material.*

 Generally, electronic authentication requires a secure electronic technique that allows the user of the technique to authenticate the identity of information associated with a sender of the document and to determine that the document was not altered during its transmission or web site posting. Sufficient electronic authentication would permit the public to know the date an electronic document is published by the state and the source or author. Such tools as watermarking serve the functions of stationery in the print world, and digital keys or digital signatures require sophisticated registration and passwords to ensure a document read on line is the one the author intended for consumption.

1. **Digital Watermarking**

Digital watermarking is the process of embedding information into a visible or invisible digital mark which may be used to verify its authenticity or identity. Digital watermarks are generally installed on software programs that help identity a document’s authentication that is created by software. Placing these marks on electronic documents prove the authenticity of the documents, when displayed to the public. However, digital watermarking is not without security concerns. As people who have been subjected to fake web sites that purport to be operated by a trusted bank or insurance company know, visible digital watermarks can be easily replicated or closely matched that could lead to public confusion and increase public scams. Fraud artists could develop identical or substantially similar watermarks and intentionally or unintentionally project documents that appear to be official.

 The digital version is not always an equal substitute for the custom paper used by many state bodies that contains a unique colored watermark to prove authenticity. This watermark is generally the state seal, and many people recognize the paper used and the watermark contained on the paper as a symbol of authentication. A digital watermarking converted to print can be reproduced on any type of paper because the watermark will be imbedded in the electronic document itself and not on paper. How is a judge presented with a printout from a state UELMA-authenticated document in court to know whether it is accurate or authentic? UELMA can cause confusion that undermines faith in the digital documents and interferes with orderly development of evidence and legal authority in litigation. This could result in judges relaying on incorrect documents, leading to bad judicial rulings.

1. **Digital Stamp**

A digital stamp is an image that is downloaded on a computer and placed on an electronic document to prove authenticity and integrity. A digital stamp is usually an electronic signature, but can also be a symbol. In order to use a digital stamp, the certificate associated with the digital signature is current (not expired), the signing person or organization is authorized to use the digital stamp by the publisher, and the certificate associated with the digital stamp is issued to the signing publisher by a reputable certificate authority (CA). If any one of these elements is absent, the document that is produced will not be considered authentic.

 Valid signatures require digital stamps that are not expired. Like driver’s license, there is an expiration date and a renewal period for certificates. Also, there are only a limited number of persons with authority to place such stamps on documents because the registration for the digital signature requires the disclosure of the individuals that will use the digital stamp.

 When using digital stamps, states must retain personnel that monitor changes in the certificate’s expiration or renewal dates, add or delete authorized users from the certificate, and constantly track the company that issues the certificate because if the company goes out-of-business, all documents using an issued digital stamp thereafter could be scrutinized for authenticity.

 While secure in use, digital stamps can present many logistical challenges. Issuers, for example, cannot easily help users to replace lost passwords. Time-consuming procedures are required for a user who has lost the pathway to a signature, or who replaced the computer that held the identification, to recover the stamp.

 The UELMA presents no criteria on how states should design either watermarks or digital stamps. The UELMA is silent on how a state should select a certificate authority provider for authorization to use such digital stamps. It does not address what happens if an issuer goes out of business or is unable to support the stamps in the future, possibly locking information out of access for a period of time, or forever. Still in relative infancy as a technology, digital security will require a new level of expertise by courts, legislatures and others, at significant public expense, if the partners to the uniform law are expected to live up to their obligations of trust in achieving the law's goals. Both authentication methods are expensive to adopt and maintain because state personnel will constantly have to monitor its implementation, address users concerns and questions, and deal with software updates and computer compatibility issues.

 *(b) If another state has adopted an Act substantially similar to this [Act], legal material in an electronic record designated as official and authenticated by that state is presumed to be an accurate copy of that legal material.*

 The very purpose of a uniform law is to require states to perform substantially the same actions in order ensure the consistent outcomes, so that each state or each user is not required to independently investigate the law, policies or products being used in commerce. In this case, the intent of UELMA is to make sure researchers, lawyers, judges and citizens doing online research into statutes or case law can trust the authenticity of the information they find. But with little specification on key elements of achieving, UELMA not only falls short in helping states understand their obligations, it deprives reciprocal states and their citizens of the ability to challenge accuracy and authenticity. The UELMA should not dictate that reciprocity requires a presumption of authenticity and accuracy until technology is more secure, costs of use are lower and means of testing compliance are better understood. The burden of disproving the basis of trust is too heavy to be borne. If courts start to question the authentication of legal material published in other states because a state’s method of authentication is inadequate--or even misunderstood-- confidence in the quality of authority will quickly erode.

**II. Preservation Problems**

 UELMA at best should provide that printed materials remain preferable when at all possible, while digital technologies and practices mature. At the least, it should require that all electronic material is published in print backup copies for preservation, and distributed to publicly available locations. Publishing in lower cost venues than books--such as in an official record newspaper--could provide an essential backup. Legal material published in print would ensure that there is no tampering or altering of information, and that the information would be preserved.

 To adequately archive electronic information, states must continuously monitor whether the computer hardware, operating systems and reading devices are available to interface to the necessary storage devices to read the preserved information. Whenever a physical medium, a storage device type, an electrical interface or a data format is being abandoned by the computer or software producers or both, preserved information dependent on the abandoned element must be converted immediately to the new standard in order to ensure preservation. The cost to hire and retain someone to monitor changes, along with the cost associated with software and computer upgrades is inestimable, because the number of changes over time is unknowable.

 Moreover, the preservation of legal material on the Internet is also filled with risks. The average life of an Internet page is about 100 days.[[1]](#footnote-1) Continuous investment is necessary to keep a web page alive. Internet site domain names require renewal or they will expire. Versions of software are engineered to require updating of material. Links become broken, and user-directories lost over time. And, given that virtually all technologies are the creatures of private enterprise, the chances that an entity will simply go out of business and leave its history to unknown and uncaring heirs is ever present.

 **III. No Set Schedule for Information Updates**

 The UELMA is without any set schedule or requirements that states must follow to provide updated or new electronic information to the public. This simply means that when a publisher of electronic information produces the information, the process time for states to receive the information or when states should make the information available to the public is at the leisure of both the publisher and state. With the UELMA silent on the number of days a state has to update legal material, users increase the risk of relying on outdated information. UELMA does not even require the web site to inform the user of the dates of postings. There is simply no way for a user to be on alert that material may have been superseded by information not yet posted.

**IV. No self-compliance provision**

 The UELMA does not have a self-compliance provision. Once a state passes the UELMA, there is nothing within the UELMA that would require the state to monitor its implementation, success, or failure. The UELMA must contain a provision that mandates a state release continued reports of its implementation and the report should be easily available to the general public.

**V. Conclusion**

 The uniform law moves next to the American Bar Association for endorsement. The ABA House of Delegates, formed primarily by state and local bar associations, will take action in February. Also, the ULC is working on an enactment plan to push the UELMA in various state legislatures.

 UELMA addresses important and needed issues in the future of digital law systems. Clearly, states abandoning the safe and known world of print for their laws are walking in the wild frontier. UELMA suggests critical goals to minimize the risk.

 But what UELMA does not do is provide states with the information either to perform their own obligations or understand the adequacy of performance of other compact states. It simply requires presumptions that goals have been achieved. Presumably, out of an abundance of caution in avoiding the suggestion of frightening cost for compliance, or overwhelming complexity in using the Internet for legal materials, the UELMA drafters have satisfied themselves that common sense and good fortune will create the right outcomes.

 At best, UELMA should be approached as a model law. It is aspirational in nature. It does not fill in the blanks that states need in order to achieve the law's goals. More work must be done, and greater maturity of the digital world must transpire before web sites can be trusted to fill responsible roles as legal publishers. But UELMA does suggest important paths for states to follow in moving into a digital world. The essential element for consideration of the proposed law is not to expect it to achieve more than it is capable of achieving. States should maintain their printed copies if at all possible, and use UELMA to guide in development of supplementary publication.

1. “Old Dominion U. professor is trying to save internet history” Washington Post 17 July 2011 [↑](#footnote-ref-1)