The E-FAC: One Year Later

by Jennifer Wondracek

In the middle of October 2012, a former student came to my office and asked me what the “FAR” was. I immediately thought of the Federal Acquisition Regulations, but this was a Florida publication. After some research, I found out that the Florida Legislature had changed the name of the Florida Administrative Weekly to the Florida Administrative Register (FAR) as of October 1, 2012. The legislature also made further changes to the publication content and frequency. The biggest change of all, however, was switching the official format of the Florida Administrative Code (FAC) from print to electronic.

This article opens with a brief history of the evolution of the FAC and FAR from print to electronic. Next, the issues that arise when legal materials, especially official legal publications, migrate from print to electronic formats are examined. State projects to digitize official legal materials and the Uniform Electronic Legal Materials Act (UELMA) are discussed, as well as the consequences, both positive and negative, of moving the FAC and FAR online. Solutions to the negative consequences are also addressed.

Brief History of the Florida Administrative Code and Florida Administrative Register

The Florida Legislature created the biannual Florida Administrative Code and the monthly Florida Administrative Register in 1961 through the enactment of the Florida Administrative Procedures Act (APA). The purpose of this act was “to set forth a uniform method of procedure under which each administrative agency will be obligated to operate so as to afford the regulated individual the fundamental guarantees insured to him [or her] by the federal and state constitutions.” In 1974, the legislature replaced the 1961 law with a more modern version of the APA, which changed the frequency of the updates to the FAC to monthly. The 1974 APA also renamed the FAR to the Florida Administrative Weekly (FAW) and required it to be issued on a weekly basis. Afterwards, the FAC and FAW were fairly stable publications for a long period of time, with minor modifications.

Efforts to turn the FAC and FAW into electronic versions began about 10 years ago. In 2004, the legislature changed the frequency of the FAC to a “continuous revision system,” eliminating a set period, such as one month or year, for revisions to the FAC. This can be difficult to implement in a print system due to the constant need to print and ship updates. The legislature created the electronic version of the FAW (E-FAW) in 2006. The electronic FAC (E-FAC) followed in 2008. In 2012, the legislature took a major leap into the digital world, making the E-FAC and E-FAW the official versions and making the print versions optional. The 2012 act also renamed the FAW back to the Florida Administrative Register. Both publications are now “continuous revision and publication[s].” There were several reasons for the 2012 changes: 1) a more efficient government, 2) reduced workload for the Department of State, and 3) to “streamline information.” Florida Department of State Legislative Affairs Director Christie Burrus also mentioned that several publications of the Administrative Codes and Registers Section of the National Association of Secretaries of State “indicated that states were moving toward continuous publication of their registers, and an electronic copy of both the Register and Code, as the official version.”

THE FLORIDA BAR JOURNAL/JANUARY 2015 19
Authentication is an issue that should be familiar to attorneys. Every time an attorney prepares for a trial, he or she must carefully build up the necessary information, such as proof of the chain of custody, to authenticate pieces of evidence that the attorney wants to enter into the record.

**Issues with Electronic Legal Materials in General**

Authentication is an issue that should be familiar to attorneys. Every time an attorney prepares for a trial, he or she must carefully build up the necessary information, such as proof of the chain of custody, to authenticate pieces of evidence that the attorney wants to enter into the record. This is an issue important enough to attorneys and courts that the rules of evidence at the federal and state levels contain rules dealing with what is needed to prove authenticity. Unfortunately, electronic versions of state laws have not received the same scrutiny.

What does authentication mean? According to the American Association of Law Libraries’ “State-By-State Report on Authentication of Online Legal Resources,” an authentic legal resource is:

one whose content has been verified by a government entity to be complete and unaltered when compared to the version approved or published by the content originator. Typically, an authentic text will bear a certificate or mark that conveys information as to its certification, the process associated with ensuring that the text is complete and unaltered when compared with that of the content originator. An authentic text is able to be authenticated, which means that the particular text in question can be validated, ensuring that it is what it claims to be.

To break this down, authenticated legal resources need to:

- Be a replica of the original text approved by the lawmaker;
- Be verified by the government as accurate and unchanged; and
- Bear some way for the viewer to confirm the government’s verification. Print resources are fairly easy to authenticate. Governments either publish their own books or nominate a specific publisher to publish the “official” source of the law. These official print sources are generally considered to be authentic due to their enduring and unchangeable nature. Online resources, however, do not have the same attributes.

Today, it is quite common to hear about someone hacking a website and changing the words; even governments are not immune. For instance, on November 15, 2013, Reuters reported that the group Anonymous had hacked multiple government websites as early as December 2012 and retained access until October 2013. The agencies included the U.S. Army, Department of Energy, Department of Health and Human Services, and possibly more. With approximately 30,000 websites being hacked each day, and government websites making up 23 percent of those hacked, it is only a matter of time before Florida’s legal websites are compromised.

As it is right now, the public, including the 98,217 attorneys licensed to practice in Florida, will be unable to see if the hackers have changed any of the language in the documents on the hacked site.

According to Matthew S. Novak, Authentication of online information is especially important for primary source material, such as court opinions, statutes, and executive documents, as these materials form the base of the legal system. And, if online publication replaces the print resource as the official source for a given title, the issue of authenticity is that much more important, as “the disappearance of print official legal sources without an authentic online substitute critically erodes the bedrock of trustworthy statements of the law.”

Because they are, in essence, self-authenticating, electronic legal documents issued or adopted by governments need an extra layer of technology to prove their authenticity, and this need will only increase as time passes and cybercriminals obtain better technology.

There are many ways to authenticate documents, and no one way is the “right” way. For instance, the California Office of Legislative Counsel undertook a study of several different authentication methods and their costs, on which they reported in December 2011. The types of technologies discussed include:

- Secure web sites
- Document hashes (digests)
- Digital signatures: self-signed and public key infrastructure (PKI)
- Certificates
- Proprietary solutions
- Visual signatures

It is beyond the scope of this article to detail all of these technologies and how they can be integrated into an authentication procedure. A brief overview of a legal document authentication program that has been successful over time, underlying the U.S. Government Printing Office’s (GPO) Federal Digital System (FDsys), may be helpful to generate a vision of a complete process.

The GPO has been discussing
authentication for over a decade. In 2007, the GPO launched a beta test of an authentication certificate program, using the 110th Congress Public & Private Laws, which were made available on GPO Access. Since then, the GPO has progressed to a full-blown authentication program with federal government documents made available on their document portal, FDsys. The technologies used by the GPO to ensure the integrity and authenticity of documents are “digital signatures on PDF files, cryptographic hash values in metadata, evidence of the trusted digital repository through the FDsys archive and access platforms, and demonstration of chain of custody.”

While perhaps a bit simplified, the GPO authentication process takes the following basic steps:

1. **Steps While Posting Documents:**
   - GPO applies a unique identification number to each document, referred to as a cryptographic hash.
   - Once a document has been stamped with its cryptographic hash, it is uploaded to FDsys, an advanced, permanent archive of federal documents that is reviewed by external auditors to verify that it meets the Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC) published by The Center for Research Libraries, National Archives and Records Administration, and the Online Computer Library Center.

2. **Third-Party Action:**
   - The user requests a document from FDsys.
   - Completed After Request (seems instantaneous):
     - A digital signature is appended to the document, which verifies the document’s authenticity. If the signature is missing or another symbol is showing, the user needs to take additional steps to verify the document’s authenticity.

7. **The requested document is sent to the user.** All of the information about the document and its authentication process, which is referred to as the chain of custody, is embedded in the document. A reader can access this information through the digital signature and the authentication stamp on the document.

In short, an authentication process for legal documents must be well thought out, able to be replicated on a large scale, and produce consistent authenticated documents whose integrity is able to be verified. While not an easy or simple process, it provides end users, such as attorneys, judges, and the general public with trustworthy legal materials, a necessity for the legal system to continue uninterrupted.

Another very important aspect of
While not one of the three essential criteria for digital preservation listed by GPO, it is vital that multiple copies of files be kept in different locations and on different hardware, in order to prevent loss due to hardware failure or disaster. In 2013, the Federal Emergency Management Agency (FEMA) recorded 62 “major disaster declarations” across the country.


Preservation is more than simply storing data. “The goal of preservation is to maintain an information asset so that it is readily accessible for use, no matter what format it was originally in, and ensuring that it is authentic and reliable by preventing such things as tampering, accidental corruption of files, media degradation, and losses through software and hardware obsolescence.”\(^{25}\)

Most people have seen the effects of the lack of preservation in their daily lives: photographs that fade, crease, and tear; VHS tapes that no longer work due to age or a broken VCR; ink on old letters or school papers fading or blurring due to water damage; paintings and even wall paint that fade and discolor due, in part, to light exposure. While the degradation of our own items may hurt us personally, the degradation of legal materials hurts society now and in the future. A prime example arose August 11, 2014, when the Office of the U.S. Courts removed digital access via PACER of documents from four appeals courts and one bankruptcy court due to incompatibility with its new case management system.\(^{26}\) As of the time of this article’s completion, closed cases filed in the 11th Circuit Court of Appeals prior to January 1, 2010, are no longer available online.\(^{27}\)

Many people are digitizing items to preserve them, but even digital items need special preservation. Most computers no longer contain 3.5" floppy disk drives, but how many files are still stored on this media, for which Sony alone once had record sales of 47 million disks in one year?\(^{28}\) Hard drives fail frequently and lose data. Older file formats that are no longer used or supported, such as Microsoft Works’ .wks, .wbs, and .wps formats, may hold essential information that is difficult to access.

What is needed to set up a proper preservation policy? The GPO provided three main criteria for digital preservation in its white paper:\(^{29}\)

- **Systematic Movement of Intact Documents to Newer Storage Media, or “Refreshment”** — As previously stated, hard drives and other storage media frequently fail. Cloud storage provider Backblaze has been tracking the longevity of their almost 28,000 hard drives and found that 5.1 percent fail in the first year of use, with the failure rate increasing to 11.8 percent after three years.\(^{30}\) Backblaze also disclosed that some brands last significantly longer than others. For instance, annual failure rates for Seagate drives ranged between 3.8 percent and 25.4 percent, whereas Hitachi annual failure rates were 0.9 percent to 1.5 percent.\(^{31}\) Thus, the drive brand and type must be carefully selected.

During the refreshment process, the documents must be moved intact so that all content is transferred and accessible. Document integrity should be a fundamental goal.\(^{32}\)

- **Regular Checks on Format Type to Determine When Conversions are Needed to Function with Newer Technology, or “Migration”** — Just as Microsoft Works formats have gone by the wayside, so too will our current digitization formats. It is important to make sure that files are maintained in modern formats that can be accurately rendered with the current technology. This is a process that must be regularly reviewed since technology changes so frequently and one may not be able to use files even a few generations older. For instance, when word processing software WordStar 2000 was released, it was not compatible with older versions, meaning that migration needed to take place quickly. Since 1993, Adobe has released eight major versions of the PDF format and at least 15 specialty types, including the long-term preservation formats, the PDF/A family.\(^{33}\) In today’s world, PDF/A-3, last updated in 2012, is the current standard for digital document preservation.\(^{34}\) As quickly as PDF formats change, at two years old, PDF/A-3 is aging and could be replaced at any time.

- **Emulation of a Working Technological Environment that will Allow a User to View the Content of the Document as Originally Intended** — According to GPO, in order of preference, the desired outcomes of the digital preservation processes are:
  - Faithfully duplicated files, rendered using the original application.
• Files which faithfully reproduce content, behavior, and presentation of the original, rendered using other software than the original application.
• Files which exactly convey the content, but may alter behavior and/or presentation, rendered using other software than the original application.32

Thus, having a technological environment that emulates the original environment and renders the document as close to the original as possible is ideal. While content is ultimately the most important element, seeing the document as originally published provides context and possibly additional information.
• Bonus Criteria: Keep Multiple Copies in Different Locations — While not one of the three essential criteria for digital preservation listed by GPO, it is vital that multiple copies of files be kept in different locations and on different hardware, in order to prevent loss due to hardware failure or disaster. In 2013, the Federal Emergency Management Agency (FEMA) recorded 62 “major disaster declarations” across the country.36 The National Fire Protection Association reported that U.S. firefighters responded to approximately 1,375,000 fires in 2012, which resulted in $12.4 billion in property damage.37 According to the “Economic Impact of Hurricane Sandy Potential Economic Activity Lost and Gained in New Jersey and New York” report prepared by the U.S. Chamber of Commerce, Office of the Chief Economist, “[i]n New Jersey alone, nearly 19,000 small businesses sustained damage of $250,000 or more with total business losses estimated at $8.3 billion as a result of Hurricane Sandy, about 1.0 percent of New Jersey Gross State Product in 2012.”38 With these statistics in mind, it is easy to see why keeping copies of electronic legal documents, especially official documents, in multiple locations is critical to a preservation policy and to society as a whole.

Members of the library community have long recognized how critical multiple copies are to their patrons. Created in 1999 at Stanford University Libraries, the LOCKSS (Lots of Copies Keeps Stuff Safe) system is a group of libraries and publishers that maintain multiple copies of digital content in order to preserve the documents and make them available should the originals become unavailable.39 There is a global LOCKSS network, which is open to almost any library. Additionally, there are private LOCKSS networks as well, which are more limited in scope, such as the Federal Depository Library Program’s LOCKSS Docs, which focuses on preserving web-based government documents.40 The State Library and Archives of Florida participated in a multi-state pilot project for digital government documents called the Florida Persistent Digital Archives and Library System (PeDALS).41 Due to staffing and funding issues in 2009, Florida discontinued its participation.42

There are many standards that may be applied to preservation, accessibility, and authentication, such as the Federal Digitization Guidelines Initiative,43 American National Standards Institute guidelines,44 the International Standards by the International Organization for Standardization,45 and the Open Archival Information System Reference Model.46 Regardless of what standard is followed, it is important that a plan be created, maintained, and followed when large-scale digitization projects, such as online legal materials, are contemplated.

Current State Legal Material Digitization Projects
As of May 1, 2014, 16 states have considered legislation to impose authentication, preservation, and accessibility standards on their online legal materials.47 Of those 16, nine states have actually enacted such laws: California, Colorado, Connecticut, Idaho, Hawaii, Minnesota, Nevada, North Dakota, and Oregon.48 All of these states passed the Uniform Electronic Legal Materials Act (UELMA),49 or a modified version thereof.

UELMA is a uniform law created by the Uniform Law Commission (ULC) that covers official legal documents. According to the ULC:

[UELMA] provides states with an outcomes-based approach to the authentication and preservation of electronic legal material. The goals of the authentication

---

[Image of Speckin Forensic Laboratories advertisement]

---

[Image of UFLLA website advertisement]

---

[Table of contents]

---

[Footer: THE FLORIDA BAR JOURNAL/JANUARY 2015 23]
and preservation program outlined in the act are to enable end-users to verify the trustworthiness of the legal material they are using and to provide a framework for states to preserve legal material in perpetuity in a manner that allows for permanent access.59 UELMA requires the state to specify what legal materials are covered under its act. The uniform act provides for the four basic categories of legal materials: constitution; legislation; reported court opinions and court rules; and agency rules, regulations, and orders.59 The state has the discretion to add other legal categories, such as legislative and agency documents.52 Under §3 of UELMA, the documents must be designated as official and published electronically after the effective date of the state’s legislation. UELMA requires the state to take three actions:

1. Authenticate the documents so that the user may verify that the document is unaltered and accurate;53
2. Preserve the documents, including maintaining multiple copies54 and
3. Provide permanent public access.55

One benefit to this act is found in §6, which provides that a document that has been authenticated is presumed to be accurate. This presumption applies both to in-state documents and to the documents of other states that have passed UELMA or similar legislation.58 While the comment to §6 explicitly states that this section does not affect the rules of evidence, including certification rules, the recognition of accurateness should only help attorneys seeking to submit electronic versions of official legal documents.

UELMA is also technology neutral. It leaves how to implement the required actions to the state and focuses instead on the outcomes. According to the act’s prefatory note:

Giving states the flexibility to choose any technology that meets the required outcomes allows each state to choose the best and most cost-effective method for that state. In addition, this flexible, outcomes-based approach anticipates that technologies will change over time; the act does not tie a state to any particular technology at any time.57

The Hague Conference on Private International Law has come to similar conclusions as to what is needed for official electronic legal materials. The Hague Conference produced the “Guiding Principles to be Considered in Developing a Future Instrument” in 2008.59 This document calls for nations to make their electronic legal materials freely accessible in an authoritative form.59 It also calls for nations to engage in long-term preservation of the legal materials.60 In March 2009, a Hague Conference Note was published that called for a new Hague Convention on improved access to electronic legal materials and cross-border cooperation with legal information and question inquiries.61

The Current E-FAC and E-FAR

• The Good — E-FAC and E-FAR have some great advantages over the print versions. The most important one is the ease of access. When print copies are the official version of a set of laws, users either need to own a copy, visit a law library, or use unofficial copies, which are not guaranteed to be correct. Most people, including attorneys, opt for the latter, using what they presume to be trustworthy sources of unofficial laws, such as LexisNexis and Westlaw databases. Having the official version in electronic format makes it much easier for people to access the information.

The Florida Legislature also made sure that the E-FAC and E-FAR are available to everyone by requiring the publications to be available for free.58 This removes many barriers to this information for those who may not be able to afford expensive legal databases. A computer or mobile device and Internet access are still required. However, as of June 30, 2012, 245,203,319 U.S. residents, or 78.1 percent of the U.S. population, had used the Internet.62 There are 120,991 libraries in the U.S.,63 including between 1,500 and 2,000 law libraries.64 With 2,000 or fewer law libraries in the U.S., it is easy to see why residents prefer the Internet.

Finally, F.S. §120.55(1)(e)1 mandates permanent retention of the FAR by the secretary of state, but not the FAC. F.S. §257.05 requires all state agencies to deposit copies of “public documents” with the State Library and Archives of Florida. According to Liz Cloud, a librarian at the State Library and Archives of Florida, the
digital version of the FAC has been archived in its original Microsoft Word format since 2006. Copies of former print FAC pages are also available, but the State Library and Archives does not guarantee that all of the pages for every year are currently available.

- The Bad — Unfortunately, there are also problems with the E-FAC and E-FAR in their current formats. First, the E-FAC is published and archived in Microsoft Word format. This format was intentionally selected because it “was determined the MS Word format would be the most universal and easiest to use.” While this format is easily opened by most end users, it is also VERY easy to change, either by a hacker or the end-user. With this current format, there is no way for a reader to verify that the information is authentic and accurate. This arises due to lack of authentication procedures.

Caitlin Murray, legislative assistant to Florida Senator Jeff Brandes, sponsor of the 2012 act, stated that authentication and preservation measures were not contemplated when drafting this act, nor was any consideration given to changing the file format for the FAC. Senator (then Representative) Brandes’ desire to make the law accessible and streamlined is very admirable. Unfortunately, there were a few elements missing from the implementation.

Interestingly, the E-FAR is published in PDF format. While still not authenticated, PDFs are more difficult to modify without the changes being obvious. This trait makes PDFs a better choice for authenticated electronic legal documents. The reason why two different formats were chosen by the state is unknown, despite efforts to discover this information.

Another issue, especially for anyone trying to build a case, is that there is no indication of how current the law is on the E-FAC and E-FAR website, https://www.flrules.org/. The only dates are the copyright date, currently listed as 2010, and the effective dates of the rules. There is no “last updated” date or “current through” indication. As all attorneys know, it is essential to verify that you have the most current version of the law, unless you are working with a historical version. If you are looking at an online regulation with an effective date of July 1, 2006, how do you know that it is the most current version of the regulation, unless you can verify when the database was last updated? Must users now provide a “last viewed” citation for the Florida administrative regulations?

The E-FAC/E-FAR website is also missing information for what is often referred to as the scope of the database, or what a user can expect to find when using the FAC and FAR databases. Generally, the scope includes information about the database, such as the name of the publisher, the correctness of the information, the frequency of updates, and a description of the documents contained within the database. This type of information is easily found in other legal resources, such as the “i” buttons in LexisNexis and Westlaw. Some of this information is available on the frequently asked questions page of flrules.org, but not all.

While the legislature considered the availability and cost of the database, they did not consider the preservation and permanent accessibility of the documents. As mentioned above, the E-FAC is being archived in Microsoft Word. No steps have been taken to make sure that as the technology ages, the files will be migrated to new formats. Presumably, when Florida was a partner in the PEDALS LOCKSS plan, these were issues that were discussed, but no plan to implement these procedures was discovered, and no law mandates such a plan or its implementation. With the fickleness and fragility of online materials, preservation, and not just archiving, needs to be a priority for official electronic documents, including the E-FAC and E-FAR.

Overall, the E-FAC and E-FAR have some great qualities, but the legislature and Florida Department of State still have some work to do.

Potential Solutions

The E-FAC should be changed to PDF or other format acceptable for authentication purposes. This format will not only work well with future authentication and preservation measures, it will also give current users a bit more assurance that the file can be relied upon until the full measures are implemented.

A “current through” or “last updated” date should be set up for each publication. It is not difficult to add these dates to a website. It can be automated or manually changed every time the publication is updated. The copyright date should also be updated, unless the state decided to
give up its copyright to flrules.org as of 2010. Making these changes would improve the ability to provide accurate citations to the courts and other entities with better confidence in their accuracy.

Scope information about the databases should be easy to add. The information need only be added once and can be located either on the frequently asked questions page or on a new page. Recommended information to provide includes when documents were first added to the database, how often the data is updated, when the data was last updated, what kind of information is included in the database, and which agencies are represented. After its addition, users will be better able to tell if the databases meet their needs.

Longer term, the Florida Legislature should consider adopting UELMA. The act will provide general guidelines for the authentication, preservation, and accessibility for all state laws for which the electronic version is designated as the official version, beginning with the E-FAC and E-FAR. The Florida Legislature and Department of State can learn from the errors and successes of the other states that have already passed UELMA and from the GPO. As seen in the section “Issues with Electronic Legal Materials in General,” the literature on the various ways to create an authentication system is growing rapidly, and should provide a good basis for a Florida system. The process of setting up these procedures may not be easy or cost-free, but the benefits of such a system would be worth the effort.

Conclusion
The digital era is here now and cannot be avoided. The digitization of primary law is already well under way. More and more states will body of law. Legislators now need to step up and commit to providing the best, most secure, authenticated permanent access to government-issued or adopted electronic legal materials for their constituents.

1 1961 Fla. Laws 538.
3 1974 Fla. Laws 952.
4 2004 Fla. Laws 2239, 2271.
6 2008 Fla. Laws 1086, 1100.
7 2012 Fla. Laws 759, 762.
9 Telephone interview with Caitlin Murray, legislative assistant to Florida Senator Jeff Brandes (Feb. 26, 2014).
10 Email from Christie Burrus, legislative affairs director, Fla. Dept. of State, to Jennifer Wondracek, head of E-Services and Technology, Univ. of Fla., Levin Coll. of Law (April 17, 2014) (on file with author).
16 Fla. Bar, How many lawyers are licensed to practice law in Florida?, Frequently Asked Questions About the Florida Bar, Jan. 1, 2014, http://www.floridabar.org/tb/faqbarwesf/63014d554d40a385256af4f00e956847fcaaf415a11d28525602606c8b5d0openDocumentHow%20many%20lawyers%20are%20licensed%20to.

26 THE FLORIDA BAR JOURNAL/JANUARY 2015