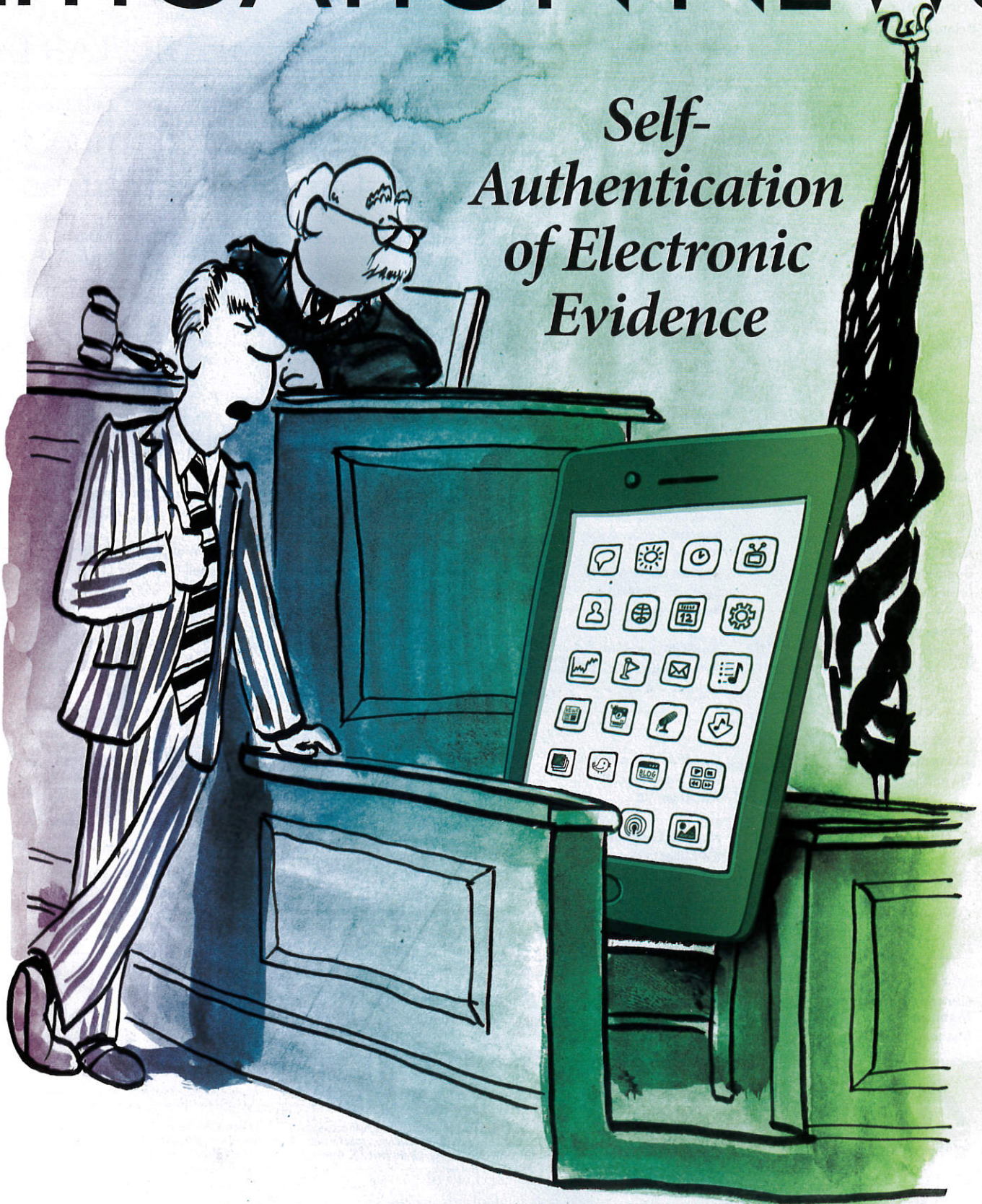
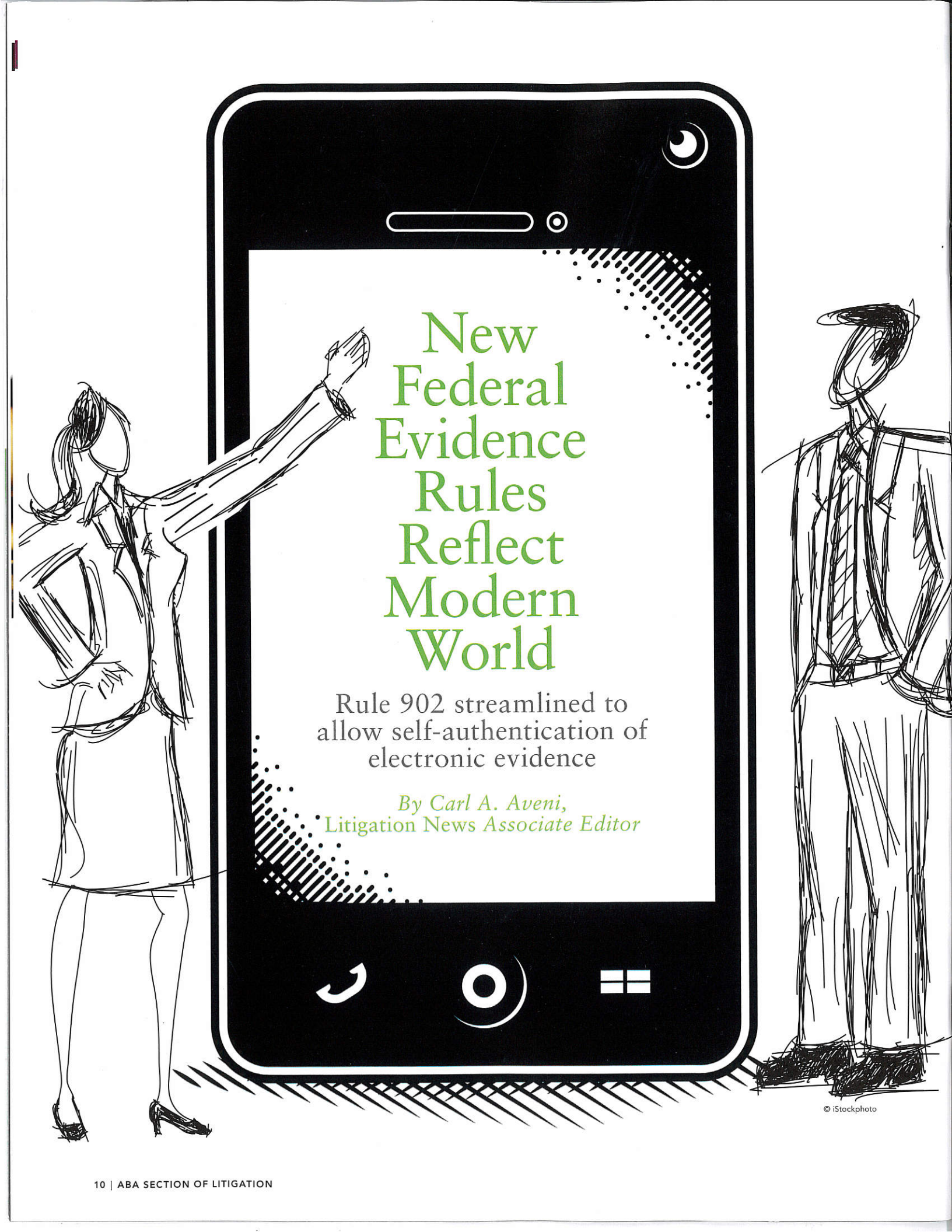


LITIGATION NEWS

Self- Authentication of Electronic Evidence



ALSO INSIDE #MeToo | SEC's Whistleblower Program

A large, black-outlined smartphone frame dominates the center of the page. Inside the frame, the title 'New Federal Evidence Rules Reflect Modern World' is written in green. Below it, a subtitle in black reads 'Rule 902 streamlined to allow self-authentication of electronic evidence'. At the bottom of the frame are three white icons: a curved arrow, a circle with a dot, and a square with two horizontal lines. To the left of the frame, a stylized line drawing of a woman in a suit points her right hand towards the title. To the right, a stylized line drawing of a man in a suit stands with his hands behind his back. The background of the frame is white, with a pattern of black dots and lines in the top right and bottom left corners.

New Federal Evidence Rules Reflect Modern World

Rule 902 streamlined to
allow self-authentication of
electronic evidence

*By Carl A. Aveni,
Litigation News Associate Editor*

It has become cliché to observe that electronic evidence has changed every aspect of modern trial practice. From smartphones, to email, to Facebook, we each leave an electronic trail of our daily lives scattered across servers, hard drives, and the cloud. No wonder litigants and their lawyers have come to rely on that data to prove or refute the crucial elements of their cases. In criminal practice, it might be GPS locations bouncing off repeaters near the crime scene. In a divorce, it might be that flurry of late-night text messages. In trade secret litigation, look for those megabytes of data that the employee downloaded right before quitting. Whatever the case, the proof at trial is now more likely to be digital than tangible.

This shift to new forms of evidence, however, has added complication, uncertainty, and inconsistency to previously settled notions of admissibility. How do you authenticate a byte? How do you prove that electronically stored data was accurately identified, collected, stored, and presented at trial? Counsel and courts alike struggle with the reliability of screenshots, or how to verify a data dump.

Into that mix, the Federal Rules of Evidence have brought a solution. As amended, Rule 902 now provides that certain machine-generated data and forensically collected electronic evidence are self-authenticating, no longer requiring a live witness to authenticate under the traditional methodology of Rule 901.

SOMETHING OLD, SOMETHING NEW

Historically, authentication has been the purview of Rule 901 and has generally required a live witness at trial, affirming that the evidence is what it purports to be based on personal knowledge or appropriate inspection. Under Rule 902, however, certain types of evidence have long been recognized as bearing sufficient intrinsic “evidence of authenticity” as to be self-authenticating, thus requiring no live witness to take the stand. These self-authenticating documents include certified copies of public records under Rule 902(4), published newspapers and periodicals under Rule 902(6), trade inscriptions affixed in the course of business per Rule 902(7), commercial paper under Rule 902(9), and certified domestic or foreign business records, following an opportunity for inspection and challenge per Rules 902(11) and (12).

Under the new amendments, Rule 902 has been updated to add two new categories of self-authenticating documents. First, under Rule 902(13):

Certified Records Generated by an Electronic Process or System. A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of 902(11).

Then, under Rule 902(14):

Certified Data Copied from an Electronic Device, Storage Medium, or File. Data copied from an electronic device, storage medium or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of 902(11).

In both instances, provided that the proponent offers an appropriate certification following an inspection and opportunity for challenge during pretrial, these new forms of electronic evidence are self-authenticating and “require no extrinsic evidence of authenticity in order to be admitted.”

Anthony J. Carriuolo, Fort Lauderdale, FL, cochair of the Social Media & Website Subcommittee of the ABA Section of Litigation’s Business Torts & Unfair Competition Committee, agrees with the logic of self-authenticating electronic evidence. “This approach makes sense for hard drives, flash drives, as well as data stored in copy machines, fax machines, and other commonly used devices that register a history of activity—that data is not really subject to human manipulation, and is the type of

routinely generated data where the accuracy of it is highly reliable.”

The committee notes for the amended Rule 902 makes the same case, in more technical terms:

Today, data copied from electronic devices, storage media, and electronic files are ordinarily authenticated by “hash value.” A hash value is a number that is often represented as a sequence of characters and is produced by an algorithm based upon the digital contents of a drive, medium, or file. If the hash values for the original and copy are different, then the copy is not identical to the original. If the hash values for the original and copy are the same, it is highly improbable that the original and copy are not identical.

Thus, identical hash values for the original and copy reliably attest to the fact that they are exact duplicates. This amendment allows self-authentication by a certification of a qualified person that he or she checked the hash value of the proffered item and that it was identical to the original. The rule is flexible enough to allow certifications through processes other than comparison of hash value, including by other reliable means of identification provided by future technology.

In sum, technological advances have made it possible to forensically confirm that electronic evidence has not been manipulated prior to trial, making the in-court verification of that same fact through a formal authentication process redundant.

STREAMLINING THE WITNESS LIST

By eliminating the need for a formal authentication process at trial, Rules 902(13) and 902(14) dispense with authentication witnesses brought to trial on wholly uncontested

issues. As the committee notes explain, “the amendment sets forth a procedure by which parties can authenticate certain electronic evidence other than

“For the last 10 years or so, we’ve been wringing our hands over how to admit social media at trial.”

through the testimony of a foundation witness. As with the provisions on business records in Rules 902(11) and (12), the Committee has found that the expense and inconvenience of producing a witness to authenticate an item of electronic evidence is often unnecessary." The notes continue:

It is often the case that a party goes to the expense of producing an authentication witness, and then the adversary either stipulates authenticity before the witness is called or fails to challenge the authentication testimony once it is presented. The amendment provides a procedure under which the parties can determine in advance of trial whether a real challenge to authenticity will be made, and can then plan accordingly.

There are other advantages as well, says Marcus R. Chatterton, Birmingham, AL, chair of the Social Media Subcommittee of the Section of Litigation's Intellectual Property Litigation Committee. "This is a little corner, sort of a nook or cranny, where we can shave off some of the challenges to electronic evidence being authenticated and admitted. Authentication was never supposed to be a high hurdle, but there have been cases where, because everybody was fighting about data collection methods, you could spend a full trial day bickering about the authenticity of digital evidence. It was pretty wasteful," he added. "The new rule is meant to fix that."

Carriuolo agrees. "The amendments should reduce the cost of evidentiary presentation. It's expensive and time-consuming—witness fees, subpoena fees, and the time folks spend sitting around at trial waiting to just authenticate evidence. A primary purpose of this rule is to eradicate that expense, recognizing the now commonplace nature of the computerized data at issue."

SETTING A NEW STANDARD

Section leaders cite additional advantages. Kirsten R. Fraser, Columbus, OH, newsletter editor for the Section's Trial Evidence Committee, believes that by creating a stable and predictable pathway to authentication, the Rule 902 amend-

ments will improve electronic data collection in discovery. "I don't think that this is going to lead to an avalanche of new electronic evidence coming into the courts," she explains, "because I think that we're already experiencing that right now. But these amendments are going to affect the quality of the collection methods that lawyers use," she predicts. "These rule changes provide an incentive for attorneys to work with certified forensic experts and standardize the way that this type of evidence is collected, preserved, reviewed, and then presented in court."

The advantages could be significant: "Having standard processes across the board helps to set expectations for your practice and for your clients," Fraser observes. "You can work that into the budget; you can build that into your discovery requests. So the collection methodology becomes regularized."

Chatterton concurs, particularly seeing benefits in the preservation and presentation of digitized social media. "There's always been sort of a do-it-yourself method of preserving and authenticating social media," Chatterton laughs. "We've done it using paralegals and project assistants who literally just downloaded photos and prepared an affidavit and stood ready to testify, laying the same kind of basic foundation you would use in authenticating a picture at trial. Now we have one more reason to skip past that and rely on a self-authenticating forensic capture through a certified professional. We can have someone who is forensically trained do the capture, and not have to worry about any sort of live authentication or authenticity challenge whatsoever." Nor will the lawyers be the only ones who benefit. "This will be a boon for e-discovery vendors, particularly those working in that social media space, specializing in forensically sound captures," Chatterton expects.

He adds, "social media evidence is already a huge part of litigation and these rules will only increase that. Twenty to 25 years ago, lawyers were wringing their hands over how they could introduce emails at trial. For the last 10 years or so, we've been wringing our hands over how to admit social media at trial. Rules

like this will make it second nature and a routine part of trial, which means we'll have to worry less up front about whether we'll get it in."

Fraser agrees, anticipating that over time, the amendments will become not only standard practice but virtually compulsory as the primary approach to digital evidence collection. "The new rules are going to drive us toward a new

"I don't think that the new rules are going to be a perfect silver bullet. But it's a good start."

standard that everyone is going to have to comply with, and at a certain point, it may be seen as an ethical duty." As she explains, "it's already an ethical duty now, for example, to use litigation holds to save electronic information. If you don't keep up with advancing technology, including in electronic

document collection and preservation, you open yourself up to ethical charges for not staying on top of it."

AUTHENTICATION IS ONLY THE FIRST STEP TOWARD ADMISSIBILITY

That said, authentication is only the first step in getting electronic evidence admitted. As the committee notes to amended Rule 902 explain, "[a] certification under this Rule can establish only that the proffered item has satisfied the admissibility requirements for authenticity. The opponent remains free to object to admissibility of the proffered item on other grounds—including hearsay, relevance, or in criminal cases the right to confrontation."

The notes illustrate the practical evidentiary issues that remain:

For example, assume that a plaintiff in a defamation case offers what purports to be a printout of a webpage on which a defamatory statement was made. Plaintiff offers a certification under this Rule in which a qualified person describes the process by which the webpage was retrieved. Even if that certification sufficiently establishes that the webpage is authentic, defendant remains free to object that the statement on the webpage was not


placed there by defendant. Similarly, a certification authenticating a computer output, such as a spreadsheet, does not preclude an objection that the information produced is unreliable—the authentication establishes only that the output came from the computer.

Chatterton sees this as opening the future battleground for admitting electronic evidence. “I can envision scenarios where under Rule 902(14), we did this forensically sound capture, we’ve got all these instant messages, here’s one message from Employee A to Employee B, but we still have to establish that Employee A was really the one controlling the account at that time. So, from that perspective, I don’t think that the new rules are going to be a perfect silver bullet. But it’s a good start.”

Even so, Carriuolo sees other advantages to using the new self-authentication procedure. “To the extent you can

get a certification from the qualified person to address the authenticity issue, you’ve, by definition, saved some time and some effort. But perhaps even better, you could use this to flush out any qualification concerns that your opponent may have as to the person who’s your declarant or your certifying person.”

Carriuolo notes that the rule amendments require the opposing party to render any objections to the certifying person in advance of trial. “Arguably, if they fail to object to the qualified person that you’re using under 902(13) or (14) to authenticate materials, you’re already one step into the courtroom in terms of having a qualified person for other purposes regarding that same data. So you might be able to use this as a kind of mini-*Daubert*. Your opponent having failed to challenge the qualifications of the certifying person on pure authenticity or the data capturing procedures that they followed, might help you priming the well for all of the other purposes for which you might still want to call this witness at trial.”

Such tactics notwithstanding, Fraser sees these amendments as an incremental improvement rather than a revolutionary change. “At the end of the day, authentication is a low bar. Relevant documents are going to find their way in. Whether it’s under the new rules or the old rules, or even if you just bring someone in to take the stand and say ‘this is mine.’ One way or another, you’ll get it in.” 

RESOURCES

- ② Fed. R. Evid. 901, available at <https://bit.ly/LN433-FRE-901>.
- ② Fed. R. Evid. 902, available at <https://bit.ly/LN433-FRE-902>.
- ② Ian S. Clement, “Webpage Held Not Self-Authenticating,” *Litigation News*, Vol. 40, No. 1 (Fall 2014), available at <https://bit.ly/LN433-Clement>.
- ② Kelso L. Anderson, “Admission of GPS Evidence Signals Brave New World,” *Litigation News*, Vol. 39, No. 3 (Spring 2014), available at <https://bit.ly/LN433-Anderson>.

2018 SECTION ANNUAL CONFERENCE

MAY 1-4, 2018 | Hilton San Diego Bayfront | San Diego, CA



Connect with leading litigators and judges from across the nation.

Register now at ambar.org/sac2018

