THE ILLINOIS ASSOCIATION OF DEFENSE TRIAL COUNSEL
IDC QUARTERLY

Feature Article

Donald Patrick Eckler
Pretzel & Stouffer, Chartered, Chicago

Ashley S. Koda
SmithAmundsen LLC, Chicago

Getting Better Every Day: The Recent Amendments to FRE 902

The ubiquity of technology has led to electronic evidence becoming increasingly the norm in litigation. Creative attorneys use Facebook posts, tweets, Fitbit data, Amazon Echo Alexa voice recordings, and GPS and Google Maps data as evidence in support of their legal and factual theories. In recent years, attorneys have used various methods to introduce such data, including the business records exception contained in Federal Rules of Evidence 902(11) and (12), and judicial notice.

In December 2017, two subsections were added to Federal Rule of Evidence 902, allowing for the self-authentication of electronic evidence. Fed. R. Evid. 902(13), (14). The purpose of this amendment was to avoid "the expense and inconvenience of producing a witness to authenticate an item of electronic evidence" that is rarely subject to a legitimate authenticity dispute. Fed. R. Evid. 902(13) advisory committee notes. The practical implication of these amendments is that parties no longer have to call a witness to lay a foundation for electronic evidence.

While Illinois has not yet adopted these subsections, the trend in litigation toward e-discovery, electronically stored information (ESI), and the use of digital evidence indicates that soon, litigators in Illinois state courts may also be able to take advantage of the relaxed authentication standards for electronically generated data.

Historical Context

Courts have come a long way in their acceptance of computer-generated evidence. In 1999, a federal district judge in Texas looked unfavorably upon the internet, writing:

> While some look to the internet as an innovative vehicle for communication, the Courts continue to warily and wearily view it largely as one large catalyst for rumor, innuendo, and misinformation. . . . Anyone can put anything on the Internet. No web-site is monitored for accuracy and *nothing* contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the court holds no illusions that hackers can adulterate the content on *any* web-site from *any* location at *any* time. For these reasons, any evidence procured off the internet is adequate for almost nothing…

St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 774-75 (S.D. Tex. 1999) (emphasis in original). Arguably, the same can also be said about physical documents. In fact, six years after the Texas judge belittled the

internet, a district court in Washington D.C. wrote that the possibility of alteration "does not and cannot be the basis for excluding ESI as unauthenticated as a matter of course, any more than it can be the rationale for excluding paper documents." *United States v. Safavian*, 435 F. Supp. 2d 36, 38 (D.D.C. 2006). The Advisory Committee on Evidence Rules cited this statement in its Memorandum to the Committee on Rules of Practice and Procedure when it sought final approval of the amendments to Rule 902.

The New Rules

At first glance, Rules 902(13) and 902(14) appear to be quite similar; however, as discussed below, the two rules serve different purposes. Rule 902(13) governs machine-generated information, whereas Rule 902(14) applies to copies of data taken from electronic devices. The full text of the new rules is as follows:

> The following items of evidence are self-authenticating; they require no extrinsic evidence of authenticity in order to be admitted:
>
> . . .
>
> **(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 Rule 902(11).
>
> **(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 Rule 902(11).

Examples of how Rule 902(13) can be used include proving that a person accessed an internet site from a specific location (such as Casey Anthony allegedly searching the internet on her home computer to find ways to murder her daughter); that a person was at the scene of the accident when it occurred (through GPS data); or that a plaintiff was actually jogging instead of recovering in bed (discovered through Fitbit data). *See e.g. Report to the Standing Committee, Advisory Committee on Evidence Rules*, 6-8 (May 7, 2016). Rule 902(13) can potentially even be used to prove that a defendant was at home during the time of a crime by accessing Amazon Echo's Alexa data, which would reveal that Alexa recorded his voice on tape at that time and date.

Rule 902(14) is slightly different in that it is intended to be used when introducing *copies* of electronic data into the record. One example is a defendant's cell phone records. Other examples could include computer-generated printouts of temperature data from a cryogenic freezer to show when that freezer's temperature climbed above cryogenic levels, or actual copies of a plaintiff's Fitbit logs.

If the distinction between the rules seems slight, that is because it is. The Federal Magistrate Judges Association made this observation when commenting "that some electronic information might be authenticated under either Rule

902(13) or (14), but that '[a]s a practical matter, the distinction may not make a difference because both types are handled in the same way.'" *Report to the Standing Committee, Advisory Committee on Evidence Rules*, Tab 2B (May 7, 2016).

There is no shortage of ways for crafty attorneys to build their cases using electronic data. With the introduction of these new rules, using electronic evidence in the courtroom is now easier than ever. "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." Fed. R. Evid. 902(13) advisory committee notes.

Certification and Notice

While the process for authenticating electronic evidence has been streamlined by the inclusion of Rules 902(13) and (14), certain constraints still apply.

First, parties introducing electronic evidence under the new rules must produce certification containing the same information to establish authenticity that a foundational witness would present on the stand. Under this rule, foreign certifications are allowed as long as they comply with the requirements set forth in Rule 902(12) governing the certification of foreign records of a regularly conducted activity. Comments to Fed. R. Evid. 902(13). While certification satisfies the requirement for authenticity, an opponent may nevertheless object to the evidence on grounds of hearsay, relevance or, in criminal cases, the confrontation clause.

Of particular importance is the difference in certification between Rules 902(13) and (14). The certification for Rule 902(13) (depending on the type of electronic evidence the proponent seeks to certify) would require something to the extent of "a description of how the operating system records information in the registry…the process by which the information recorded produces an accurate result, and how the evidence (presumably a printout of registry information) accurately reflects information stored in the registry." Busen, Carry, It's the End of Authentication (of ESI) as We Know It, Discovery Advocate, BakerHostetler (Nov. 29, 2017), https://www.discoveryadvocate.com/2017/11/29/its-the-end-of-authentication-of-esi-as-we-know-it/.

In contrast, the certification under Rule 902(14) is more technical. Without getting into the details, data copied from an electronic device contains a "hash value." If the copy of the evidence is identical to the original, the "hash values" of the original and copied data will match. Therefore, to certify a copy of data obtained from an electronic device, the qualified person signing the certification need only state that he or she compared the hash values and found that they matched.

Second, the party introducing the evidence must provide reasonable notice of their intention to opposing counsel. Rules 902(13) and (14) reference Rule 902(11) which establishes the notice requirement: "Before the trial or hearing, the proponent must give an adverse party reasonable written notice of the intent to offer the record—and must make the record and certification available for inspection—so that the party has a fair opportunity to challenge them." Fed. R. Evid. 902(11). This shifts the burden of going forward onto opposing counsel.

Attorneys should take note that a "challenge to the authenticity of electronic evidence may require technical information about the system or process at issue, including possibly retaining a forensic technical expert." Fed. R. Evid. 902(13) advisory committee notes. Therefore, challenges to authenticity should not be made unless there is reason to believe that the evidence is fraudulent or otherwise unreliable.

Hearsay

While these amendments streamline the authentication process and make the authenticity of electronic evidence more difficult to challenge, hearsay rules continue to apply. Interestingly, the Advisory Committee on Evidence Rules recently considered (but ultimately declined to approve) "a proposal that would add a hearsay exception, intended to address the phenomenon of electronic communication by way of text message, tweet, Facebook post, etc." Advisory Committee on Evidence Rules, *Minutes of the Meeting of April 17, 2015* (New York, New York, April 17, 2015). The Committee reasoned that these types of electronic communications are unreliable and an "ill-fit for the standard hearsay exceptions." *Id.* However, the Advisory Committee did note that it will continue to monitor the issue of "eHearsay," especially considering the success of Wisconsin's "recent perception" exception as applied to eHearsay ("Wisconsin state judges [are] generally satisfied with the application of the recent perceptions exception and its application to eHearsay.") *Id.*

Social media postings and text messages suffer from the same hearsay problems as spoken and traditionally written words. Assume that a plaintiff in a car accident case posts on Facebook minutes after the accident describing the incident and stating that she feels perfectly fine. At the time of trial, plaintiff's counsel would certainly want to keep this post out but a savvy defense attorney would be aware of the hurdles surrounding the admission of this evidence and how to tackle them.

The defense attorney would have to establish the authenticity of this post —according to the Advisory Committee on Evidence Rules, authenticity of social media posts can be established through the poster's testimony that she did in fact post the comment; evidence that the Facebook account belonged to the plaintiff; and circumstantial evidence such as the plaintiff's customary use of emojis or that the post has the same writing style as the plaintiff. *See* Hon. Grimm, Paul W. and Joseph, Gregory P, *Best Practices for Authenticating Digital Evidence*, 9 (2016). Defense counsel could also attempt to subpoena the plaintiff's smartphone records (including IP data, date and time information, and GPS coordinates) and hire a forensic expert to testify that this statement was, in fact, posted from the plaintiff's cell phone at the place and time that the accident occurred. While this would establish the authenticity of the records, defense counsel would still likely face a hearsay exception.

Here, defendant would argue that the Facebook post is not being admitted for the truth of the matter asserted, but rather the simple fact that the plaintiff posted a Facebook status despite allegedly being in debilitating pain. Defense counsel could also argue that the statement falls under the hearsay exception for then-existing mental, emotional or physical condition. Ill. R. Evid. 803(3). Thus, while the process of authenticating electronic evidence is different from authenticating traditional documents and records, the hearsay exceptions remain traditional in their application to electronic statements.

Practice Pointers for Illinois State Court

Until Illinois adopts the new amendments, Illinois attorneys should be cognizant of other methods available for introducing electronic evidence. In particular, if opposing counsel refuses to stipulate to the authenticity of electronic evidence, attorneys may continue to use typical authentication principles, the business records exception where applicable (such as emails sent and received in the course of a regularly conducted activity), or move the court to take judicial notice of certain websites and data.

THE ILLINOIS ASSOCIATION OF DEFENSE TRIAL COUNSEL
IDC QUARTERLY

Typical Authentication Principles

Under Rule 902, official publications, newspapers and periodicals, and business records are self-authenticating. Fed. R. Evid. 902(5), (6), (11) and (12). This remains true for *electronic* publications, newspapers, and business records found on the internet. Therefore, in these circumstances, no authentication issue arises. However, hurdles arise when attempting to authenticate Facebook posts, tweets, and Google Maps street views. In those instances, attorneys need to find creative ways to introduce the evidence.

As discussed above, social media postings can be authenticated via circumstantial evidence. The Manual on Best Practices for Authenticating Digital Evidence contains a list of methods by which an attorney can authenticate the author of an email. Many of these methods can equally apply to social media postings: the author's name or nickname is in the post; the post discusses facts only the purported author or small subset of individuals would know; the author's customary use of emojis or emoticons; and reference to facts uniquely tied to the author (*e.g.* family members' contact information). Hon. Grimm, Paul W. and Joseph, Gregory P, *Best Practices for Authenticating Digital Evidence*, 9 (2016).

Judicial Notice

Sometimes an attorney may want to introduce evidence of a Google Earth street view image to show what the scene of a car accident looked like at or near the time of the incident. For example, a car accident occurs on November 12, 2016 near a construction site at the intersection of Clark Street and Division Street. The savvy attorney types the intersection into Google Earth and discovers that the street view image was taken on November 10, 2016, and does, in fact, show a construction zone. While the attorney can authenticate the Google Earth image by subpoenaing Google's custodian of records to testify at trial, there is an easier way.

Asking the court to take judicial notice of a fact found on a website is one way to streamline the introduction of electronic evidence without the benefit of the new Rule 902 amendments. Under Illinois Rule of Evidence 201,

> A judicially noticed fact must be one not subject to reasonable dispute in that it is either (1) generally known within the territorial jurisdiction of the trial court or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot be questioned.

In recent years, courts have taken judicial notice of information found on government and public websites, the distance between places on Google Maps, Google Maps street views and (to the great chagrin of the Texas court that disparaged the internet) even facts found in Wikipedia articles. *See generally* Bellin, Jeffrey and Ferguson, Andrew Guthrie, *Trial by Google: Judicial Notice in the Information Age*, 108 Nw. U. L. Rev. 1137 (Summer, 2014).

THE ILLINOIS ASSOCIATION OF DEFENSE TRIAL COUNSEL
IDC QUARTERLY

Conclusion

Every day, electronic data becomes more embedded into our daily routines. It is only a matter of time before Illinois and other state courts adopt Federal Rules of Evidence 902(13) and (14). In fact, the influence of the internet is so strong that eHearsay may even become an exception to the general hearsay rule. But in order to take advantage of the new amendments which allow the self-authentication of electronic evidence with a certificate, attorneys need to be mindful to carefully and accurately collect such evidence through the life of a lawsuit. This will ensure that attorneys will be able to make the proper certifications envisioned by these amendments.

As has already been observed, the electronic evidence affected by the new rules is rarely subject to authenticity disputes. Thus, the new rules bring with them countless benefits to both sides— they will streamline the authentication process, reduce the costs of subpoenas, witness, and travel fees, and shorten the length of trials. Clients will save money and courts will save time.

About the Authors

Donald Patrick Eckler is a partner at *Pretzel & Stouffer, Chartered*, handling a wide variety of civil disputes in state and federal courts across Illinois and Indiana. His practice has evolved from primarily representing insurers in coverage disputes to managing complex litigation in which he represents a wide range of professionals, businesses and tort defendants. In addition to representing doctors and lawyers, Mr. Eckler represents architects, engineers, appraisers, accountants, mortgage brokers, insurance brokers, surveyors and many other professionals in malpractice claims.

Ashley S. Koda is an associate at *SmithAmundsen LLC* and a member of the firm's Aerospace and Commercial Litigation Practice Groups. Ms. Koda represents clients in aerospace, commercial and manufacturing industries, handling issues stemming from premises liability, product liability, aviation, municipal liability, and business disputes. Ms. Koda earned her J.D., *cum laude*, from Chicago-Kent College of Law. While in law school, she worked as a law clerk at an insurance defense firm, as a Judicial Extern for the Honorable Franklin Valderrama of the Circuit Court of Cook County, and as an intern for Chicago-Kent's Criminal Defense Clinic. Additionally, she was the recipient of the CALI Excellence for the Future Award for her performance in Complex Litigation.

About the IDC

The Illinois Association Defense Trial Counsel (IDC) is the premier association of attorneys in Illinois who devote a substantial portion their practice to the representation of business, corporate, insurance, professional and other individual defendants in civil litigation. For more information on the IDC, visit us on the web at www.iadtc.org or contact us at PO Box 588, Rochester, IL 62563-0588, 217-498-2649, 800-232-0169, idc@iadtc.org.