45 No. 1 Litigation 6

Litigation
Fall, 2018

Litigator's Toolbox

Column

From the Bench

Hon. Paul W. Grimm[a1]

NEW EVIDENCE RULES AND ARTIFICIAL INTELLIGENCE

WESTLAW LAWPRAC INDEX

JUD--Judicial Management, Process & Selection

Imagine this situation: Jane Jones applied for a senior programmer vacancy advertised by Digital Solutions Inc. Her résumé boasts undergraduate and graduate degrees in computer science, 15 years of successful programming experience in a series of increasingly demanding programming jobs, and annual job performance evaluations of "always exceeds expectations" or better.

The job went to Bill "Slacker" Bailey instead of Jane. His résumé shows that he took various computer-related courses for two years at a community college, but never obtained an associate degree, and gained five years of job experience as a tech-support specialist at a local big-box electronics store and another 10 years as the founder of "HakkersPlace," an online blog devoted to computers and programming.

Jane filed a Title VII gender discrimination case against Digital in federal court. The essence of her claim is that she is demonstrably better qualified than Slacker and that by giving the job to him, Digital discriminated against her on the basis of her gender.

Digital vehemently denies that discrimination played a role in Slacker's selection and asserts that despite her more impressive résumé, Jane was the *lesser*-qualified candidate. In support of its defense, Digital disclosed during discovery that it retains a company by the name of WorkerMatch to help it find the best candidate for each of its job openings. According to Digital, WorkerMatch has developed a computer analytics method of identifying the most qualified applicants for any particular job vacancy.

Here is how it works: WorkerMatch asks Digital to identify the top-performing employees doing the same type of work as is required for the job vacancy. Then, for a time, it digitally monitors how they perform their jobs. Next, the employees participate in a far-ranging online interview about not only how they do their jobs, but also their interests, hobbies, use of language, and mannerisms.

Then, using a computer program that incorporates an artificial intelligence (AI) algorithm, WorkerMatch analyzes the recordings of the high-performing Digital employees and develops an online questionnaire tailored to the needs of the particular Digital job vacancy. All job applicants must complete the questionnaire; those who score well then participate in an online video-recorded interview.

Again using the AI algorithm software, WorkerMatch compares the applicants' questionnaire responses and online interview results against the results of questionnaire responses and recorded interviews of Digital's top performers. The software then prepares a rank-ordered list of the 10 most qualified candidates.

Digital engaged WorkerMatch to help fill the vacancy for which Jane applied. Digital's human resources director and vice president of programming reviewed the list of the top 10 candidates that WorkerMatch provided and selected the top 5 for personal interviews. Slacker was ranked number 2, Jane number 9.

Because Jane wasn't in the top 5, she was not interviewed in person. Slacker occupied the number 2 spot--he interviewed in person and was the clear choice of the majority of the Digital hiring team. So he got the job.

To support its defense, Digital has produced copies of the job candidate analysis done by WorkerMatch. Those records corroborate Digital's explanation of how Slacker was picked over Jane. But during a Rule 30(b)(6) deposition of Digital's corporate designee--its human resources director--Digital was unable to provide any details about *how* WorkerMatch's AI analytics worked, explaining that it relied on WorkerMatch to develop the selection process. Digital added, however, that since using WorkerMatch, all the employees hired were doing a terrific job.

In its court filings, Digital has argued that it cannot be liable for ***7** intentional gender discrimination because the selection process was designed by WorkerMatch's computer analysis, not by anyone at Digital, and that an inanimate computer cannot form discriminatory intent. In response, Jane's attorneys filed a motion in limine to exclude the documents generated by WorkerMatch, arguing that Digital cannot prove how the AI algorithm used by WorkerMatch functions and therefore cannot show that the software was not programmed to make gender discriminatory selections.

The hearing on the motion in limine is only a week away. How is Digital to overcome Jane's challenge to the admissibility of the records generated by WorkerMatch regarding the hiring of Slacker over Jane?

If you think this hypothetical is farfetched, think again. As it happens, AI analytics already is being used by companies to make employment decisions. *See, e.g.*, Stephen Buranyi, *Rise of the Racist Robots--How AI Is Learning All Our Worst Impulses*, Guardian, Aug. 8, 2017, www.theguardian.com/inequality/2017/aug/08/rise-of-the-racist-ro-bots-how-ai-is-learning-all-our-wors-timpulses; Daniel Newman, *Your Artificial Intelligence Is Not Bias-Free*, Forbes, Sept. 12, 2017, www.forbes.com/sites/danielnewman/2017/09/12/your-artificial-intelligence-is-not-bias-free/#1a3f331cc783; Josh Constine, *Pymetrics Attacks Discrimination in Hiring with AI and Recruiting Games*, Tech Crunch, Sept. 20, 2017, https://techcrunch.com/2017/09/20/unbiased-hiring/.

This has raised concern about whether computer programs using AI to make hiring selections have discriminatory criteria embedded within them. When faced with evidentiary challenges to decisions based on AI analysis that was not developed by the hiring company, how can the hiring company prove that the methodology used is reliable? Must it produce the developer of the AI program as a witness at a hearing or trial?

That could be difficult, not to mention expensive. The users of AI software created by others likely do not have direct control over the availability of the witness (or witnesses) who developed the computer program. Is there any alternative to requiring live testimony in every case in which computer analysis underlies the process that is central to the key issue in the case?

Two New Evidence Rules

As of December 1, 2017, the answer is yes! This is because two new federal rules of evidence became effective on that date--Rule 902(13), covering certified records generated by an electronic process or system, and Rule 902(14), covering certified data copied from an electronic device, storage medium, or file.

These new rules may greatly facilitate the authentication of electronically generated evidence in federal cases. And because digital information increasingly plays an important role in both civil and criminal cases, lawyers need to know about them and how to use them.

Both are located in Federal Rule of Evidence 902, which sets out examples of evidence that is self-authenticating--meaning that "they require no extrinsic evidence of authenticity in order to be admitted." This is vital to understanding their importance. If you do not need "extrinsic evidence"--read: "witnesses"--to authenticate the evidence, then it comes in on its own. And that is when the potential savings in time and expense can be considerable.

Rule 902(13), "Certified Records Generated by an Electronic Process or System," provides:

> 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) [is self-authenticating]. The proponent must also meet the notice requirements of Rule 902(11). [Rules 902(11) and 902(12) permit the self-authentication of certified copies of domestic and foreign business records.]

Rule 902(14), "Certified Data Copied from an Electronic Device, Storage Medium, or File," states:

> 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) [is self-authenticating]. The proponent also must meet the notice requirements of Rule 902(11).

The 2017 advisory committee note to Rule 902(13) explains its purpose succinctly:

> The amendment sets forth a procedure by which parties can authenticate certain electronic evidence other than 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 ***8** unnecessary. 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.

Rule 902(13) has several important features. First, while it satisfies the authentication requirement of Rule 901(a), it does not address other potential evidentiary issues such as hearsay or the original writing rule. *See* Paul W. Grimm, Daniel J. Capra & Gregory J. Joseph, *Authenticating Digital Evidence*, 69 BAYLOR L. REV. 1, 40 (2017) ("[A] certification under the proposed rules can establish only that the proffered item has satisfied the admissibility requirements for *authenticity*. So the opponent remains free to object to admissibility on other grounds ...." (emphasis in original)). But because the greatest challenge to digital evidence tends to be authentication (*id.*), the benefits the rule provides are substantial.

Second, the required certification must be substantive, not boilerplate. That means the person making the certification must meet the Rule 602 personal knowledge requirements; the Rule 702 scientific, technical, or specialized knowledge requirements;

and the Rule 901(b)(9) requirements to explain *how* the process or system that generated the electronic record produces reliable and accurate results.

As the 2017 advisory committee note cautions,

> [a] proponent establishing authenticity under this Rule must present a certification containing information that would be sufficient to establish authenticity were that information provided by a witness at trial. If the certification provides information that would be insufficient to authenticate the record if the certifying person testified, then authenticity is not established under this Rule. The Rule specifically allows the authenticity foundation that satisfies Rule 901(b)(9) to be established by a certification rather than the testimony of a live witness.

Using the Rules

So, if you want to take advantage of Rule 902(13), you will need to carefully consider who must make the certification (which may require more than one person) and carefully draft it to ensure that it is as comprehensive as the testimony that would have to be offered at trial to meet the authentication requirement. "A declaration that satisfies 28 U.S.C. § 1746 would satisfy the declaration requirement ... as would any comparable certification under oath." FED. R. EVID. 902(11) advisory committee note (2000).

Third, Rule 903(13) requires that adversaries be given the same notice required by Rule 902(11) and (12). That means that "[b]efore 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) (2017).

The rule is silent about how much advance notice must be given, but it must be reasonable, so it is unwise to wait until the last minute to do so. Rule 902(11) does not impose any duty on the party that receives a certification under 902(13) or (14) to reciprocate by providing reasonable notice to the proponent of its objection to the sufficiency of the certification, so prudent counsel will want to make sure that she provides as much advance notice of the 902(13) or (14) certification as is reasonably possible and request that her adversary notify her of any intent to challenge the sufficiency of the certification by a reasonable date in advance of the hearing or trial. If opposing counsel does not agree to do so, ask the court to impose a deadline for notice of any challenge.

While Rule 902(13) focuses on records generated by an electronic process or system, Rule 902(14) focuses more narrowly on *data* copied from an electronic device, storage medium, or file. But the observant reader will detect a certain overlap between the two. After all, aren't copies of records produced by an electronic system or process also data copied from an electronic device?

Why the overlap? One commentary on the new rules explains it this way:

> It should be noted that there is an overlap in the two provisions. When data is copied from an electronic device, the result is a record (i.e., the copy) that is ordinarily generated by an electronic process (because the copy is generated electronically). So it is true that the electronic information that is covered by Rule 902(14) could also for the most part (but not completely) be covered by Rule 902(13). The overlap does not run very far the other way, however; that is, records generated by an electronic system may well not be a "copy" of anything. The Advisory Committee had a good reason for proposing a separate subdivision for copies of electronic data, because the process of authenticating a copy--usually through hash value--is unique and specific. Rule 902(14) is in large part directed to a fairly specific problem--cloning hard drives and offering the clone rather than the original, through a hash value match. The process of authenticating machine-generated evidence more broadly can be satisfied by

> a number of different methods. Put another way, the copying processes that serve for authentication under Rule 902(14) do only one thing--assuring that there is ***9** no change between the copy and the original.

Grimm et al., *Authenticating Digital Evidence, supra*, at 40-41.

The advisory committee explained the justification for Rule 902(14) this way:

> 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 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.

FED. R. EVID. 902(14) advisory committee note (2017).

The Distinction Between the Rules

The essential distinction between Rule 902(13) and Rule 902(14) is this: 902(13) is likely to be the "utility player" governing a wide range of situations in which machine-generated evidence is offered into evidence, while Rule 902(14) more narrowly focuses on how to demonstrate that data copied from an electronic device, storage medium, or file are identical to the original.

So, for example, you could use Rule 902(13) to prove that a USB drive device was connected to a computer (Grimm et al., *Authenticating Digital Evidence, supra*, at 42-43); that a server was used to connect to a webpage (*id.* at 43-44); where a person was at the time that a digital photograph was taken using his smart phone (using the GPS coordinates recorded by the phone on the photograph) (*id.* at 44); that there is an association between or that there has been contact between various individuals (through text message logs) (*id.* at 44-45); and, for purposes of the hypothetical that appears at the start of this article, that the AI algorithm used to rank the qualifications of the applicants for the job that Jane and Slacker applied for had the ability to select the most qualified applicant without any gender-based bias.

Given the ubiquity of the use of digital devices in all aspects of human activity, the list of potential uses of Rule 902(13) is as infinite as the uses of digital technology itself. As Rule 902(14) is narrower in scope, its most frequent use likely will be to prove that the contents of a forensic image made of the hard drive of a computer or cell phone is identical to the contents of the computer or phone from which the image was made. *Id.* at 45-46.

The narrower scope of Rule 902(14) in no way diminishes its importance, however, because evidence taken from forensic images of digital devices is introduced all the time in both criminal and civil cases. And in criminal cases, the use of Rules 902(13) and (14) could implicate the Confrontation Clause because the certifications required by the rules would appear to be "testimonial," as they clearly contemplate use at a trial.

In *Melendez-Diaz v. Massachusetts*, however, the majority opinion noted that at common law, "a clerk's certificate authenticating an official record-- or a copy thereof--for use as evidence" traditionally was admissible, meaning that "[a] clerk could by affidavit authenticate or provide a copy of an otherwise admissible record" for introduction into evidence in a criminal case without running afoul of the Confrontation Clause. 557 U.S. 305, 322-23 (2009).

That language, colloquially referred to as "the *Melendez-Diaz* carve out"-- Grimm et al., *Authenticating Digital Evidence, supra*, at 47-48--"has been relied on by every circuit court that has evaluated the admissibility of certificates offered under Rule 902(11) to provide the foundation for and to authenticate business records under the hearsay exception ... [of] Rule 803(6)" to rule that the certificates do not violate the Confrontation Clause. *See id.* at 48 (citing cases).

And because Rules 902(13) and (14) require the exact same type of certificates as Rule 902(11), it is quite likely that their use in a criminal case also would survive a Confrontation Clause challenge. *Id.* That said, until the circuit courts actually have ruled this way, a prudent prosecutor would be wise to file a pretrial motion in limine to secure an advance ruling to this effect before assuming away any Confrontation Clause concerns regarding the use of Rules 902(13) and (14) in a criminal trial.

As with any new rules of evidence, it will take some time for the usefulness of Rules 902(13) and (14) to take effect. And keep in mind that, while useful, their impact is modest. "They provide an easier method to authenticate but they do not reduce the *standards* of authentication." *Id.* at 40 (emphasis in original).

And they satisfy only the requirement of Rule 901(a) that non-testimonial evidence be authenticated before it is admissible. They do not satisfy any other evidentiary foundation that may be required.

But inasmuch as the chief problem associated with admissibility of digital information tends to be its authentication, the modest helping hand offered by Rules 902(13) and (14) promises to be very useful indeed.

Footnotes

[a1] **The author is a U.S. district judge in the District of Maryland.**

45 No. 1 LITIG 6

End of Document