ARTICLE

LAW OF THE FOAL: CAREFUL STEPS TOWARDS DIGITAL COMPETENCE IN PROPOSED RULES 902(13) AND 902(14)

Hon. John M. Facciola[*] & Lindsey Barrett[·]

CITE AS: 1 GEO. L. TECH. REV. 6 (2016)

https://perma.cc/Z9NN-ZY95

INTRODUCTION

The Federal Rules of Evidence were originally established to create uniformity in evidence law by providing guidance for every evidentiary problem that could be reasonably expected to occur at a trial. The rules are firmly grounded in the tangible, as courts typically deal with the concrete concerns posed by physical evidence or the testimony of witnesses. But, as our tangible world has grown increasingly virtual, so too has the evidence, creating a diametric switch the existing rules are ill-designed to accommodate. The rules of evidence simply do not speak specifically to the admissibility of digital evidence lawyers and judges now confront. Rules that speak to the written word, testimony, or physical evidence must now be construed and applied to electronic evidence, despite the radical differences between how most evidence was once created, and how it is generated now. The question of how and whether to adapt the rules of evidence for the digital era presents two possible approaches: Does disruptive technology compel a rewriting of existing rules, or are technology-specific approaches to evidentiary issues a

[*] U.S. Magistrate Judge (ret.); Adjunct Professor of Law, Georgetown Law. J.D. Georgetown Law, B.A. College of the Holy Cross.

[·] Managing Editor, GLTR; Georgetown Law, J.D. expected 2017; Duke University, B.A. 2014.

solution in search of a problem, and more likely to create new problems as lawyers and judges struggle to craft new rules for digital evidence?

In May 2015, the Advisory Committee on Evidence proposed Rules 902(13) and 902(14) concerning the authenticity of electronically stored information.[1] While the proposed amendments are not overly ambitious and do not tackle the issue of proof needed to establish the authenticity of all digital evidence under Rule 901, they do embrace certain technological realities that can guide courts into an updated understanding of evidence in the digital age. Rule 902(13) would provide for a certification process for digital information produced by a computer system or process, analogous to Rule 902(11)'s provision for certification of business records.[2] Rule 902(14), governing the self-authentication of copies of electronic information, would allow the authentication of a file by using its hash value, a unique identifier frequently referred to as a "digital fingerprint,"[3] obviating the need for further authentication by witness testimony.[4] The proposed Rules will likely reduce litigation costs spent authenticating information, and help foster judicial efficiency and familiarity with technology. Authentication using hash values will allow courts and lawyers to focus on more pressing issues, and will provide courts with the assurance that presented digital evidence is, in fact, what it purports to be.

The proposed new rules represent a modest step toward updating rules that were created to ensure sufficient authentication of physical documents to meet the needs of an increasingly digital evidentiary landscape. The amendments must, however, be implemented carefully, lest lawyers ignore that ascertaining the authenticity of digital evidence is only the first step in

---

[1] There are two crucial reports on these new rules: (1) Memorandum to Honorable Jeffrey S. Sutton, Chair, Standing Committee on Rules of Practice and Procedure from: Honorable William K. Sessions, III, Chair, Advisory Committee on Evidence Rules, May 7, 2015 *in* JUDICIAL CONFERENCE OF THE UNITED STATES COMMITTEE ON RULES OF PRACTICE AND PROCEDURE, STANDING AGENDA BOOK – MAY 2015, 463–473 (2015) (hereinafter May 2015 Report), http://www.uscourts.gov/rules-policies/archives/agenda-books/committee-rules-practice-and-procedure-may-2015, which provides the text of the proposed rules; and (2) Memorandum to Honorable Jeffrey S. Sutton, Chair, Standing Committee on Rules of Practice and Procedure from: Honorable William K. Sessions, III, Chair, Advisory Committee on Evidence Rules, May 7, 2016 (hereinafter May 2016 Report), http://www.uscourts.gov/rules-policies/archives/committee-reports/advisory-committee-rules-evidence-may-2016.

[2] May 2016 Report, *supra* note 1, at 10.

[3] *See* Simon Garfinkel, *Fingerprinting Your Files*, MIT TECH. REV. (Aug. 4, 2004), http://www.technologyreview.com/news/402961/fingerprinting-your-files/.

[4] *See* May 2016 Report, *supra* note 1, at 12.

determining admissibility. Difficult questions under other evidentiary rules, and in articulating the demands of the right to confrontation persist.[5] But the new rules are, at the very least, a significant start.

THE PROBLEM

The question of how to coalesce new technology with older legal frameworks has produced contradictory approaches, summarized in now-classic form by Professor Lawrence Lessig[6] and Judge Frank Easterbrook.[7] The first would take an exceptionalist approach to applying old laws to new facts, recognizing that disruptive technology frequently compels the construction of new rules to preserve the principles and objectives those rules are intended to serve.[8] The second would critique that approach as unduly hasty and apt to create conflicting, erroneous, and patchwork rules for a world changing too quickly for lawmakers to keep apace.[9] As Judge Easterbrook famously described it, "Lots of cases deal with sales of horses; others deal with people kicked by horses; still more deal with the licensing and racing of horses…[a]ny effort to collect these strands into a course on "The Law of the Horse" is doomed to be shallow and to miss unifying principles."[10] The fear of creating a well-intentioned but misguided set of new rules continues to nag lawmakers attempting to adapt existing rules to new facts.

The divide between the two approaches is keenly felt in the evolving world of digital evidence. In his book, *Foundations of Digital Evidence*, George Paul argues that the rules of evidence were premised on a philosophy of empiricism, and the rules that this philosophy generated have nothing to do

---

[5] That the report of a blood test, based on analysis of its contents using computer technology, is authentic has nothing to do with whether the result of the test is scientifically accurate, and whether the defendant should be entitled to call a human being who has certified its accuracy. *See* United States v. Washington, 498 F.3d 225, 232-234 (Michael, J., dissenting).

[6] Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 546 (1999).

[7] Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F., 207, 216 (1996).

[8] *See* Lessig, *supra* note 6, at 546.

[9] Easterbrook, *supra* note 7, at 207 ("[t]he best way to learn the law applicable to specialized endeavors is to study general rules."); *id.* at 215-16 ("Error in legislation is common, and never more so than when the technology is galloping forward. Let us not struggle to match an imperfect legal system to an evolving world that we understand poorly. Let us instead do what is essential to permit the participants in this evolving world to make their own decisions.").

[10] *Id.*

with how the modern world assesses the accuracy of its communications.[11] Paul, therefore, argues in favor of a radically different approach to the admission of digital evidence.[12] A competing, Easterbrook-sympathizing school would argue that "if it ain't broke, don't fix it," insisting that the old rules of evidence will work very well with the new technology, as they have worked with information generated by telegraph messages and Xerox machines.[13]

The digital era has therefore created a dramatic issue for courts – how to apply rules and doctrine intended for physical evidence to intangible, digital evidence. The Lessig-Easterbrook fault line divides those, like George Paul, who would completely re-conceptualize and reimagine the rules to deal with a changing evidentiary landscape, and those that want to graft the old rules onto new kinds of evidence. While the battle lines have formed, there is a stalemate. There is no perceptible movement towards the wholesale revision of the Federal Rules of Evidence to deal with digital information.[14] Like it or not, the competent lawyer will largely have to grapple with the Rules as they are, no matter how ill-fitting the applicability of the pertinent Rule and the information being offered. Nevertheless, the proposed new rules are a refreshing step towards a more modern and efficient judiciary for the Information Age.

THE PROPOSED NEW RULES

The Advisory Committee on Evidence Rules has proposed to the Committee on Rules of Practice and Procedure that the Federal Rules of

---

[11] GEORGE L. PAUL, FOUNDATIONS OF DIGITAL EVIDENCE 3, 16 (2008). In the interest of transparency, it should be noted that Judge Facciola wrote the forward.

[12] *Id.* at xxv ("We are at a crossroads— a change of phase. With our new information infrastructure, the concept of written evidence has reached a critical tipping point, Judges, professors, students, and thinkers must rewrite the rules.").

[13] Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure*, 4 NW. J. TECH. & INTELL. PROP. 171, 172 (2006), http://www.law.northwestem.edu/joumals/njtip/v4/n2/3/J.%20Withers.pdf.

[14] *See* Jonathan L. Moore, *Time for An Upgrade: Amending The Federal Rules of Evidence To Address The Challenges of Electronically Stored Information In Civil Litigation*, 50 JURIMETRICS 148 n. 9 (2010) (*citing* PAUL R. RICE, ELECTRONIC EVIDENCE: LAW AND PRACTICE 492 (2d Ed. 2008) (noting that "new evidentiary problems faced in the internet age have been directly addressed in few, if any, of these evidence codes")); George L. Paul, *The "Authenticity Crisis" In Real Evidence*, L. PRAC. TODAY, (Mar. 2006), http://www.abanet.org/lpm/lpt/articles/tch03065.shtm ("Certainly no action has been taken by Congress to change the federal rules of evidence to address the recent wave of digitization.").

Evidence be amended to add two new rules governing the authenticity of electronically stored information.[15] The proposed rules seem to be a compromise between the Lessig[16] and Easterbrook[17] schools, and recognize the novelty of this new evidence within the context of traditional evidence law. While the amendments do not deal with the substantive issues as to how digital information is authenticated under Rule 901,[18] they do accomplish two laudable goals. First, the proposed rules create a means of authentication that will relieve the proponent of calling a witness to authenticate the information, if the witness provides a certificate that this information is the product of a process or system that produces an accurate result.[19] Second, they permit a copy of electronically stored information to be admitted if a declarant indicates that she has copied that information from a device, storage media, or electronic file if it is authenticated by what the proposed rule call a "process of digital identification."[20] In the latter situation, the person who derived the copy need not testify; written certification that she made the copy will suffice.[21] More specifically, proposed Rule 902(13) provides that "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 902(11) or 902(12)."[22] Proposed Rule 902(14) provides that "data copied from an electronic device, storage media, 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 902(12)."[23]

[15] May 2016 Report, *supra* note 1, at 1.
[16] Lessig, *supra* note 6, at 546.
[17] Easterbrook, *supra* note 7, at 216.
[18] Rule 901 states that a document is not relevant unless it is what it purports to be and a party must, therefore, produce sufficient evidence to support a finding that it is what it purports to be. For digital evidence that is not self-authenticating, lawyers traditionally use three rules of evidence by: (1) providing testimony from a witness with 901(b)(1); (2) demonstrating that the appearance, contents, substance, internal patterns or other distinctive characteristics of the item, taken together with all the circumstances under 901(b)(4); (3) providing evidence describing a process or system and showing that it produces an accurate result under 901(b)(9).
[19] May 2016 Report, *supra* note 1, at 10.
[20] *Id.* at 12.
[21] *Id.*
[22] *Id.* at 10.
[23] *Id.* at 12.

Rule 902(13)

The Committee began with the proposition that in the vast majority of cases, the authenticity of electronically stored information is never challenged and it is, therefore, wasteful to insist that a witness come to court to state what is obvious and unlikely to be challenged.[24] On a daily basis, the courts admit into evidence paper documents upon the certification of a custodian, complying with the requirements of Rule 803(6) without any need to call the custodian.[25] Accordingly, electronically stored information should be admitted on the same basis. The Committee, therefore, indicated that its purpose is "narrow: to allow authentication of electronic information that would otherwise be established by a witness."[26] The opposing party, who is entitled to notice of the intention to use such a certification, remains free to challenge the representations made in the certification. The certification suffices only to excuse the witness from appearing if her certification is filed with the court and there is no objection to the authenticity of the evidence as asserted by the certification.

The Advisory Committee provides a series of helpful examples of how the new rule would operate to relieve a party from calling a witness and securing instead the necessary certification from a witness.[27] A party could establish how the iPhone software captures the date, time, and GPS coordinates of each picture taken with the iPhone, permitting the court to conclude that whoever took the picture did so at a particular time and from a particular place.[28] It bears noting that Exif data, the automatically generated metadata indicating, among other things, the date, time and place a particular photo was taken,[29] can be altered—but this is highly unlikely to be the case for the vast majority of cases, and is further counteracted by the requirement

[24] *Id.* at 5.
[25] FED. R. EVID. 803(6).
[26] May 2016 Report, *supra* note 1, at 10.
[27] *Id.* at 7-10.
[28] *Id.* at 7-8.
[29] J.D. Biersdorfer, *Erasing GPS Data from* iPhones, PERSONAL TECH, N.Y. TIMES (Nov. 7, 2016), (explaining how to remove exif data from an image file), http://www.nytimes.com/2016/11/08/technology/personaltech/erasing-gps-data-from-photos.html?ref=technology; *see also*, CAMERA & IMAGING PRODUCTS ASS'N, EXCHANGEABLE IMAGE FILE FORMAT FOR DIGITAL STILL CAMERAS: EXIF VERSION 2.3 31, (December 2012), http://www.cipa.jp/std/documents/e/DC-008-2012_E.pdf (explaining the technical standard for the inclusion of GPS tag in Exif data for digital cameras); *Id.* at 44 (explaining the technical standard for the inclusion of date and time a picture is taken in the Exif data).

that the party certify that the metadata is legitimate.[30] A party could explain how a Samsung phone logs the content date, time and communicating phone that called or was called by the Samsung phone of text messages that were sent to or from the phone.[31] In each of these instances, the certification of how the electronically stored information was created, transmitted, and stored would suffice to establish authenticity even though the witness was not called. Authenticity is further contingent on the court finding that that the electronically stored information being offered into evidence is what it purports to be (under Rule 901(a)), or self-authenticating (under Rule 902(9)) because the certification establishes that it is the product of a process or system that produced an accurate result.[32]

Rule 902(14)

The proposed rule pertaining to copies of electronically stored information, Rule 902(14), is much easier to apply. The Rule is premised on the fact that it is possible to assign a unique numerical identifier called a "hash value" to electronically stored information by performing calculations on the data within the electronically stored information. It is premised on the incontrovertible reality that each piece of electronically stored information has a unique hash value.[33] The hash value has been referred to as a digital fingerprint because it is a functionally unique and random identifier for a given set of data.[34] The hash value of a file is created when a data string (such as an electronic file serving as evidence) is run through a series of mathematical functions, resulting in a seemingly random string of characters of a fixed length, and much shorter than the input data string. [35] That output is

[30] Jason Cipriani, *How to view, remove, Exif photo data on your iOs device*, CNET (FEB. 20, 2015), https://www.cnet.com/how-to/how-to-view-remove-exif-photo-data-on-your-ios-device/ (explaining how the date and time an iOS photo was taken, and the location the photo was taken, can be removed using an app).
[31] May 2016 Report, *supra* note 1, at 8.
[32] FED. R. EVID. 902(9).
[33] *Cf.* BARBARA J. ROTHSTEIN ET AL., MANAGING DISCOVERY OF ELECTRONIC INFORMATION: A POCKET GUIDE FOR JUDGES 24 (1st ed. 2007) (defining hash value as "a unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set" and providing further background information), http://federalevidence.com/pdf/2008/09-Sept/FJC_%20Managing%20Discovery%20of%20Electronic%20Information.pdf.
[34] Garfinkel, *supra* note 3.
[35] Bret Mulvey, *Hash Functions*, THE PLUTO SCARAB, http://papa.bretmulvey.com/post/124027987928/hash-functions (last visited Nov. 23, 2016).

the hash value of the input file, which could have been anything from a simple string of characters to all the files on a hard drive.[36]

Three properties of commonly available hash functions—high collision resistance, high preimage resistance, and high second preimage resistance—make their use the ideal for the authentication of digital evidence. A hash function has a high collision resistance when it would be computationally infeasible (computer science-speak for "almost impossible") for two different inputs, computer files for example, to have the same hash value after the hash function is applied to them.[37] A hash function has a high preimage resistance when it is computationally infeasible to determine the input based on the algorithm and the hash value (such that the hash algorithm is "one-way"); and it is second preimage resistant is when it is computationally infeasible for two different inputs to produce the same hash value.[38] If one uses a hashing algorithm with the three properties mentioned above, it is overwhelmingly unlikely that two pieces of evidence will ever produce the same hash value. The odds of hashing two different pieces of evidence and getting the same hash value is on the order of one in 340 undecillion— or 300 trillion trillion—if using the popular MD5 hash algorithm.[39] Because a hash algorithm is designed to give a complex and highly random output, even a slight change in the input will result in a radically different hash value. This change could be as small as a single pixel added to an image.[40] Comparing hash values makes it easy to identify if the file has been even slightly modified.[41]

---

[36] *Id.*

[37] NAT'L INST. OF STANDARDS & TECH., RECOMMENDATION FOR APPLICATIONS USING APPROVED HASH ALGORITHMS 6, (2012), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-107r1.pdf ("The longer a hash value is, the more collision resistant it is, as the predicted collision resistance is believed to be half the length of the hash value in bits...").

[38] Mike James, *Hashing – The Greatest Idea in Programming*, I PROGRAMMER, http://www.i-programmer.info/babbages-bag/479-hashing.html (last visited Nov. 23, 2016). While collision resistance and second preimage resistance are similar, they are distinct attributes. *See Second Preimage Resistance vs. Collision Resistance*, CRYPTOGRAPHY STACK EXCHANGE, (Dec. 24, 2014), http://crypto.stackexchange.com/questions/20997/second-pre-image-resistance-vs-collision-resistance.

[39] *See* Rothstein, *supra* note 33, at 24.

[40] Stephen Hoffman, *An Illustration of Hashing and Its Effect on Illegal File Content In The Digital* Age, 22 INTELL. PROP. & TECH. L.J. 6, 10-11 (2010).

[41] Glenn Fleischmann, *Faster Computing Will Damage The Web's Integrity*, MIT TECH. REV. (Oct. 8, 2012), http://www.technologyreview.com/view/429531/faster-computation-will-damage-the-internets-integrity/.

The uniqueness of a hash value to a file, the fact that the hash value it is a compact microcosm of the larger file, and the feature that the slightest change to the input will be immediately revealed, strengthens the argument for Proposed Rule 902(14). The Committee extrapolated from the primary premise, namely that authentication using hash values is essentially error-proof, that assigning hash values to original files could provide for a more seamless self-certification process. The odds of a false positive, of the system finding a match because a different file and the piece of evidence happened to share the same hash value, are infinitesimally low.[42] Hashing provides exactly the proof that Rule 902 requires: that the document is what the attorney states that it is.[43]

Thoughtful Implementation

While the new rules eliminate the unnecessary, there is an obvious concern: Lawyers will seek the path of least resistance and will resort to forms that will simply regurgitate the new rules ("I certify that _____was the result of an accurate system or process"), and move on. But, if the once tangible has become virtual, lawyers and judges will make very little progress if they use these new rules as an excuse not to understand how the underlying technology works. They will fail to realize that the technology properly understood can lead to further advances in creating new rules that will deal with the other issues of authenticity that are based on a forensic evaluation of how computers operate, and create vitally useful information. Forensic technology may answer quickly whether a particular computer produced this electronically stored information because data created by the system itself can answer that question indubitably in particular case.[44] Unless an individual

[42] Robyn Burrows, *Judicial Confusion and the Digital Drug Dog Sniff: Pragmatic Solutions Permitting Warrantless Hashing of Known Illegal Files*, 19 GEO. MASON L. REV. 255, 258 (2011).

[43] The Committee's understanding of how hash values was not precisely correct. Describing the use of hash values for Proposed Rule 902(14), the report tells us that "[a] hash value is a unique alpha-numeric sequence of approximately 30 characters that an algorithm determines based upon the digital contents of a drive, media, or file. Thus, identical hash values for the original and copy reliably attest to the fact that they are exact duplicates." May 2016 Report, *supra* note 1, at 12. A hash value is not approximately 30 characters, and in fact the longer it is, the smaller the chance of computational collision–in other words, the more closely authentication approximates the kind of certainty the process is designed to secure.

[44] *See e.g.*, CAT3 LLC v. Black Lineage, Civil Action No. 14Civ5511 (AT)(JF), 2016 BL 7342 (S.D.N.Y. Jan. 12, 2016) (forensic evaluation of metadata proved certain crucial facts);

uses a privacy-enhancing technique like Tor,[45] user metadata indicating the time and IP address of a particular user activity took place can be stored by the company operating the application, such as Facebook or Google, or the internet service provider, such as Comcast or AT&T.[46] Should we undertake to create new rules that more precisely define when forensic evidence can permit the court to conclude that a particular piece of digital evidence is authentic? These rules are arguably only the beginning of a process that will use technological certainty as the only true premise of the authenticity of digital evidence.

Counsel also must realize that a certification of the authenticity of a result is not a certification of its correctness. There are two questions presented when, for example, the report of a breathalyzer is offered into evidence and the resolution of the first, is the report authentic, is, at best, an introduction to the second—did it work? If only the first question is asked and answered we run the risk that the new rules will be completely misconstrued. While Rule 901 speaks of authenticity, a malfunctioning machine cannot produce relevant evidence and, despite the certification, counsel still must call the scientist who performed the analysis if there is reason to doubt that result. Knowing that a report is an accurate reproduction of the results of a process or system is one thing; knowing whether that process or system worked correctly is another.

CONCLUSION

The ultimate implications of hashing for self-authenticating evidence is clear, and the steps that the Committee have taken to move towards a pragmatic understanding of how digital evidence works is promising. Hashing has presented lawyers with a strongly practical alternative to requiring certification of evidence that both computer science and basic statistics declare authentic. The other rule, which neatly equates certification of digital records with the certification of paper business records, is equally sensible and, properly used, can save the time and money spared by avoiding calling a witness who will state the obvious.

GE Netcom v. Plantronics, Civil Action No. 12-1318 (LPS), 2016 WL 3792833 (D. Del. July 12, 2016) (same).

[45] Kyle Swan, *Onion Routing and Tor*, 1 GEO. L. TECH. REV. 110 (2016).

[46] *See* Kim Zetter, *Google Takes on Rare Fight Against National Security Letters*, WIRED (Apr. 4, 2014, 1:02 PM) (explaining that internet service providers and others can store confidential records about their customers, such as subscriber information, e-mail addresses, websites visited and more).

But the ambition of these rules is humble. They do not deal with an articulation of the proof needed to establish authenticity under Rules 901 or 902, leaving significant questions of substantive proof still up for debate. Courts will, therefore, continue to apply rules truly designed for paper to electronically stored information. Nevertheless, there is reason for optimism—if the certifications are done correctly, they could illuminate for the court the underlying forensic science that will explain why the evidence being offered can be trusted and relied upon. This is, of course, a welcome alternative to lawyers and courts looking everywhere except the technological basis to determine the authenticity of an email or a Facebook entry. Finally, the use of hash values as the means of guaranteeing that one electronically stored file is the same as its copy is particularly welcome. Time spent attempting to establish that two electronically stored files are identical other than by using hash values at this juncture is inefficient in both time and cost. Rules 902(13) and (14) are an acknowledgment of the need to reform analog rules for a digital age; while a modest and careful beginning, they are at the very least a modest and careful step in the right direction.