

EDITORIAL BOARD

Editor in Chief

Andrew Doyle
doyle_andrew@msn.com

Associate Editor

James W. Satola
jsatola@roadrunner.com

Managing Editor

Lynne G. Agoston
(240) 404-6488
social@fedbar.org

Book Review Editors

Heaven C. Chee
Soledad M. Valenciano

Judicial Profile Editors

Hope Forsyth
Hon. Karoline Mehalchick

Articles Editors

Joanna Fox
Sheila Hollis
Christopher Lucca
Bruce McKenna
Anne Perry
Dalmacio Posadas
Elizabeth Turnbull
Susan Yorke

Columns Editor

Ira Cohen

Senior Proof Editor

Peter Mansfield

Proof Editors

Kristine Adams-Urbanati
Sarika J. Angulo
Ellen Denum
Sara Gold
Niles Ilich
Jeffrie Boysen Lewis
Jon Jay Lieberman
Glenda McGraw Regnart
Amanda Thom
Jeremy Stone Weber

The Federal Lawyer (ISSN: 1080-675X) is published bimonthly six times per year by the Federal Bar Association, 1220 N. Fillmore St., Ste. 444, Arlington, VA, 22201 Tel, (571) 481-9126, Fax (571) 481-9090, Email: social@fedbar.org. Subscription Rates: \$14 of each member's dues is applied toward a subscription. Nonmember domestic subscriptions are \$50 each per year; foreign subscriptions are \$60 each per year. All subscription prices include postage. Single copies are \$5. "Periodical postage paid at Arlington, VA... and at additional mailing offices." "POSTMASTER, send address changes to: The Federal Lawyer, The Federal Bar Association, 1220 N. Fillmore St., Ste. 444, Arlington, VA 22201." © Copyright 2021 Federal Bar Association. All rights reserved. PRINTED IN U.S.A.

Editorial Policy: The views published in *The Federal Lawyer* do not necessarily imply approval by the FBA or any agency or firm with which the authors are associated. All copyrights held by the FBA unless otherwise noted by the author. The appearance of advertisements and new product or service information in *The Federal Lawyer* does not constitute endorsement of such products or services by the FBA. Manuscripts: *The Federal Lawyer* accepts unsolicited manuscripts, which, if accepted for publication, are subject to editing. Manuscripts must be original and should appeal to a diverse audience. Visit www.fedbar.org/tflwritersguidelines for writers guidelines.

January/February 2021: Civil Rights Issue



34 Brick-by-Brick: The Case for Foundational Discovery

By Rebekah L. Bailey, Stephen J. Teti, and Kate A. Fisher

42 Availability of Treatment and Rehabilitation in Federal Prison: The Critical Role of the Presentence Report

By Marc Blatstein, D.P.M.; Fay F. Spence, J.D.; E.J. Hurst II, J.D.; and Maureen Baird

54 Demystifying the Civil Deposition

By John R. Byrne

62 Best Practices in Virtual Proceedings

By Rachel C. Hughey and Tara D. Elliott

66 Federal Rules of Evidence 902(13) and 902(14)—A Useful Tool for Electronic Data

By Jordi C. Martínez-Cid

1220 N. Fillmore St., Ste. 444
Arlington, VA 22201
Ph: (571) 481-9100 • F: (571) 481-9090
fba@fedbar.org • www.fedbar.org

BOARD OF DIRECTORS

PRESIDENT • W. WEST ALLEN
wwa@h2law.com
PRESIDENT-ELECT • ANH LE KREMER
anh.kremer@cdtrad.com
TREASURER • MATTHEW C. MOSCHELLA
mcmoschella@sherin.com
Ernest T. Bartol
etbartol@bartollaw.com
Jeanette M. Bazis
jbazis@greeneespl.com

Joey Bowers
jbowersfba@gmail.com
Kevin A. Maxim
kmaxim@maximlawfirm.com
Glen R. McMurry
glen.mcmurry@dinsmore.com
Hon. Karoline Mehalchick
karoline_mehalchick@pamd.uscourts.gov
Aline S. Momoh
adine.momoh@stinson.com
John R. Thomas
jrt@fed-lit.com
Jessica R. Toplin
jtoplinfba@gmail.com
Hon. Mimi E. Tsankov
(personal capacity)
mimi.tsankov@gmail.com
Christie C. Varnado
cvarnado@seibelsfirm.com
Michael S. Vitale
mvitale@bakerlaw.com

SECTION AND DIVISION CHAIRS
CHAIR, SECTIONS AND DIVISIONS
COUNCIL
To Be Appointed
ADMIRALTY LAW
Scott Bluestein
ALTERNATIVE DISPUTE RESOLUTION
Bryan J. Branon
ANTITRUST AND TRADE REGULATIONS
Vacant

BANKING LAW
Christopher Bellini
BANKRUPTCY LAW
Christopher Sullivan
CIVIL RIGHTS LAW
Robin B. Wagner
CORPORATE AND ASSOCIATION COUNSEL
David Greene
CRIMINAL LAW
E.J. Rymsza

NATIONAL STAFF
EXECUTIVE DIRECTOR
Stacy King
sking@fedbar.org
DIRECTOR OF MEMBERSHIP AND CHAPTERS
Dominick Alcid
dalcid@fedbar.org
MANAGING EDITOR
Lynne G. Agoston
social@fedbar.org

OUTREACH AND FOUNDATION MANAGER
Cathy Barrie
cbarrie@fedbar.org
OPERATIONS MANAGER
Holly Delidle
hdelidle@fedbar.org
DIRECTOR OF SECTIONS AND DIVISIONS
Mike McCarthy
mmccarthy@fedbar.org
MARKETING DIRECTOR
Jennifer Olivares
social@fedbar.org

CONFERENCE MANAGER
Caitlin Rider
crider@fedbar.org
SR. DIRECTOR OF PROFESSIONAL
DEVELOPMENT
Melissa Schettler
mschettler@fedbar.org
PROGRAM COORDINATOR
Ariel White
awhite@fedbar.org

MEMBERSHIP SPECIALIST
Miles Woolever
mwoolever@fedbar.org
VICE PRESIDENTS FOR THE CIRCUITS
FIRST CIRCUIT
Scott P. Lopez
Oreste R. Ramos
SECOND CIRCUIT
Olivera Medenica
Dina T. Miller
THIRD CIRCUIT
Christian T. Haugsby
Frank J. McGovern

SENIOR LAWYERS
Steve Miller
SOCIAL SECURITY LAW
To Be Appointed
STATE AND LOCAL GOVERNMENT
RELATIONS
Andrew S. Ballentine
TAXATION
Robert Russell
TRANSPORTATION AND
TRANSPORTATION SECURITY LAW
Steve Osit
VETERANS AND MILITARY LAW
Maura Clancy
YOUNGER LAWYERS
Anna W. Howard

COLUMNS

3 President's Message

The Constitution Empowers Us:
Federalism and Protecting Civil Rights
Through Diffused Government
By W. West Allen

5 Washington Watch

How Trump Broke the Judicial
Nominations Record
By Bruce Moyer

6 At Sidebar

Civility in Our Profession
By Hon. Karoline Mehalchick

8 Bankruptcy Brief

Bankruptcy 2004 Examinations and
Why You Want to Use Them
By Hon. Elizabeth L. Gunn and
Elizabeth G. Smith

10 Diversity & Inclusion

Reflecting on the Diversity & Inclusion
Committee's Police Liability Programs
By Kiera Murphy and
Katherine Earle Yanes

12 Focus on Indian Law

The Far End of the Trail of Tears:
McGirt v. Oklahoma
By Joel West Williams

16 FBA Outreach

Add a Judge and Stir: Chapters
Challenged to Advance Civics
Education With "Toolkit"
By Cathy Barrie

18 Commentary

Rethinking Reasonable: Recognizing a
Prisoner's Expectation of Privacy
Under the Fourth Amendment
By Bradley Taylor

22 Tribute to RBG

Heroes Never Die:
How RBG Can Live On
By Rupa G. Singh

PROFILES

24 Hon. Joan N. Ericksen

Senior U.S. District Judge, District of
Minnesota
by Jeya Paul

30 Hon. Ortrie D. Smith

Senior U.S. District Judge,
Western District of Missouri
by Steven Wolfe

BOOK REVIEWS

70 Originalism as Faith

Reviewed by Diego M. Pestana

72 Defender in Chief: Donald Trump's Fight for Presidential Power

Reviewed by Louis Fisher

74 The Year of Peril: America in 1942

Reviewed by Henry S. Cohn

DEPARTMENTS

76 Supreme Court Previews

FBA MEMBER NEWS

82 Sections & Divisions

85 Chapter Exchange

88 Member Spotlight

Federal Rules of Evidence 902(13) and 902(14)— A Useful Tool for Electronic Data

JORDI C. MARTÍNEZ-CID

Among the myriad ways the coronavirus pandemic has disrupted our lives has been how it has caused people to spend increasingly more time online or engaged with electronics, and it has forced the legal system to adapt its practices to carry out its duties in an effective manner. As a result, practitioners should be aware of the relatively new and sometimes overlooked Federal Rules of Evidence 902(13) and 902(14). These subsections deal with how litigants can authenticate certain kinds of electronic data. Given that there will presumably be more electronic data that could become evidence and that the judiciary is actively seeking how to modernize evidentiary hearings and trials, litigators should familiarize themselves with these rules because of their benefits

Federal Rules of Evidence 902(13) and 902(14) Streamline Authentication Requirements for Electronic Data

In 2017, subsections 13 and 14 were added to Federal Rule of Evidence 902. As the subsections are brief, they are included here:

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).¹

What these subsections represent is a streamlining of authentication requirements, reducing the expense and inconvenience in getting certain forms of electronic data authenticated. They seek to accomplish this by allowing a party to authenticate records generated by an electronic system or data copied from electronic devices or files without the need for a foundation witness.

Making Use of the Subsections Lends Itself to Our Current Environment

Given the paucity of cases surrounding subsections 13 and 14, they are either being underutilized² or used with very few objections from adverse parties.³ They should be used more and are particularly useful now for a few reasons. First, people in general are spending more time online and presumably creating more electronic data.⁴ Second, people are increasingly more aware of this kind of data, and this kind of data is taking on an increasing level of importance.⁵ Third, the pandemic has caused individuals and companies—which previously may have been more amenable to certifying business records or the like—to focus on more pressing needs. Now a single “qualified person,” using forensically sound methods, can certify diverse kinds of electronic data, including corporate emails, social media from different platforms, footage from surveillance devices or drones, and text messages.⁶

While there is always a practical reason for why a litigator might want to use these subsections—namely to not call a foundation witness and all that it entails—pandemic-related changes to the legal system make the subsections even more attractive. For those remaining in-person hearing and trials, the subsections allow practitioners to avoid dealing with foundation witnesses who may not be willing to expose themselves to public spaces or risk air travel under the current conditions. For remote evidentiary hearings and trials, practitioners can avoid being at the mercy of foundation witnesses and their computers, the strength of their internet connections, and their facility with video-conferencing software. And, given that the subsections require that adverse parties be given reasonable notice, lawyers will often be apprised of real disputes regarding the evidence ahead of the hearing or trial and can adequately prepare.

Complying With the Requirements of the Subsections Is Relatively Simple

One of the primary differences between the subsections is that subsection 13 allows for the authentication of data output by electronic systems, while subsection 14 allows for the authentication of copies of data from electronic systems. Despite certain courts not focusing on the differences between the subsections,⁷ parties should take precautions to ensure they are proceeding under the correct subsection. As one commentator synthesized the difference, subsection 13 deals with data generated by computers while subsection 14 deals with data generated by people.⁸

Regardless of which subsection is the correct one for the electronic data, the party needs to obtain a written certification by a “qualified person” or custodian.⁹ Self-serving declarations by counsel for the proponent of the evidence are insufficient.¹⁰ Generally speaking, a qualified person is one who understands how the data system operates and is often an IT specialist, an investigator, a forensic accountant, or a litigation support/e-discovery specialist. This qualified person or custodian should be able to attest to the following:

- They are familiar with and have requisite education or skills to use the process or system that produces the data.
- The process or system used is forensically sound and capable of producing accurate results.
- The data constitutes a “Record of a Regularly Conducted Activity” under Federal Rule of Evidence 803(6)(A)-(C).
- A jurat or declaration under oath, which may differ depending whether the evidence is a domestic or foreign record.

Ideally, the certification should be detailed, include the above declarations, and highlight steps taken to ensure reliability and accuracy.

Depending on the record retrieved, special care should be taken with regard to the metadata, which is the “structural information of a file[.]”¹¹ Metadata is different from the underlying record or data and is normally not accessible to users. It is referenced by the advisory committee notes, and courts oftentimes focus on this metadata to determine authenticity.¹² The rule also requires that the record and certification be made available for inspection and that the adverse party has “reasonable written notice of the intent to offer the record[.]”¹³

That the data is authentic does not mean that it is admissible. As the subsections only deal with the authenticity of the data, they do

not suddenly bring certain kinds of electronic data into the ambit of becoming evidence, and they do not address the ownership, control, reliability, or relevance of the evidence. The subsections address neither the accuracy of the data nor its substance, and they are not by themselves capable of overcoming a hearsay objection.¹⁴ Therefore, practitioners may want to consider whether the qualified person should address relevancy, chain of custody, and identity issues referenced in Federal Rules of Evidence 401 and 901 to arrive at the end goal of having the evidence introduced.¹⁵

Practitioners Should Pay Attention to the Rule Early and Make Greater Use of It

Parties often fail to focus on trial-related issues at the outset of a case; this is a mistake. Practitioners need to think about the collection and authentication of data as early as possible. This is particularly true given the ephemeral nature of some electronic data. Ensuring proper collection of the data can prove the difference with regard to more “modern” lawsuits, such as ones involving allegedly defamatory statements made through various social media platforms, including TikTok, that can be modified or removed in an instant. But it can also be crucial even in more “traditional” litigation cases.

For example, in a case alleging breach of contract, metadata and other electronic information showed that the defendant could not have breached the contract attached to the complaint because that contract was not in existence at the time of the supposed breach. The other party, unable to locate and authenticate the contract that was presumably in place, decided to negotiate a settlement on terms very favorable to the defendant. In other cases, the subsections have been cited to defeat assertions by criminal defendants that they had been prejudiced and could not obtain evidence from a computer database,¹⁶ and they may have been instrumental in the failure to oppose a motion to compel arbitration.¹⁷ Further, providing the certification and notice to the adverse party well ahead of an evidentiary hearing or trial can avoid unnecessary objections and litigation posturing, or could strengthen claims that the opposing party is acting in bad faith or with a misunderstanding of the facts.

As explained, Federal Rules of Evidence 902(13) and 902(14) are useful, easy-to-use tools that should form part of a federal litigator’s arsenal. The pandemic makes them all the more useful and valuable. Practitioners and parties can reduce costs and save time and effort in authenticating data using those subsections and can utilize them as offensive or defensive tools in litigation. ☺



Jordi C. Martínez-Cid is a partner in the Miami office of León Cosgrove, LLP, where he specializes in media and international litigation and arbitration. Martínez-Cid is a graduate of Yale Law School and is a former federal law clerk and a former in-house attorney at NBCUniversal. Responses are welcome. Copyright © 2020 by Jordi C. Martínez-Cid.

Endnotes

¹FED. R. EVID. 902(13)-(14).

²The author’s research uncovered only two federal circuit court opinions regarding these specific subsections and a handful of district court opinions. See *United States v. Dunnican*, --- F.3d ---, no. 19-3092, 2020 WL 3056229, at *7 (6th Cir. June 9, 2020) (discussing

the authenticity of records certified by a special agent who performed the digital extraction); *United States v. Gasperini*, 729 Fed. App'x 112, 114-15 (2d Cir. 2018) (affirming the authenticity ruling of the trial court under FED. R. EVID. 902(14)).

³Some commentators have suggested that the subsections are “regularly used” and conclude that the limited number of opinions is because the subsections “are functioning as intended.” Parties have either stipulated to authenticity, or courts have so determined in a straightforward manner. See Andrew Schupanitz and Jacklin Chou Lem, *Judges’ Treatment of Federal Rules of Evidence 902(13) and 902(14)*, 68 DOJ J. FED. L. & PRAC. 109 (2020).

⁴See Ella Koeze and Nathaniel Popper, *The Virus Changed the Way We Internet*, THE NEW YORK TIMES (Apr. 7, 2020), <https://www.nytimes.com/interactive/2020/04/07/technology/coronavirus-internet-use.html> (noting an increase in online and app usage); Marguerite Reardon, *Coronavirus transforms peak internet usage into the new normal*, C|NET (Mar. 23, 2020), <https://www.nytimes.com/interactive/2020/04/07/technology/coronavirus-internet-use.html> (noting spiking internet traffic resulting from the pandemic).

⁵See, e.g., *Knight First Amendment Inst. at Columbia Univ. v. Trump*, 928 F.3d 226 (2d Cir. 2019) (affirming a decision that the president of the United States violated the First Amendment by blocking users from accessing or interacting with his Twitter account).

⁶See FED. R. EVID. 902(13)-(14).

⁷*Compare United States v. Bondars*, No. 1:16-cr-228, 2018 WL 9755074, at *2 (E.D. Va. Aug. 20, 2020) (holding that “screenshots taken from the Internet Archive’s Wayback Machine,” which are presumably akin to computer printouts, could be authenticated under Fed. R. Evid. 902(13)), and *United States v. Zuschlag*, No. 2:16-cr-158-DBH, 2008 WL 2669957, at *4 (D. Me. June 4, 2018) (citing both sections as a manner in which data retrieved from a computer database could be authenticated), with *Rosado-Mangual v. Xerox Corp.*, No. 15-3035, 2019 WL 7247776, at *29 (D.P.R. Dec. 27, 2019) (quoting *United States v. Meienberg*, 263 F.3d 1177 (10th Cir. 2001)) (finding that computer printouts were not properly authenticated under Fed. R. Evid. 902(13) because they are “not the result of a process or system used to produce a result, but merely printouts of preexisting records that happened to be stored on a computer”).

⁸See 2 ROBERT E. LARSEN, NAVIGATING THE FEDERAL TRIAL § 9:6 (2020).

⁹FED. R. EVID. 902(13)-(14).

¹⁰See *La Force v. GoSmith, Inc.*, No. 17-cv-05101, 2017 WL 9938681, at *3 (N.D. Cal. Dec. 12, 2017) (holding that a declaration by plaintiff’s counsel that included the date, device, and browser used to obtain a webpage and screenshots, that did not include a verification that counsel had been the one that retrieved the data was insufficient for finding authenticity under Fed. R. Evid. 902(13)).

¹¹The Sedona Conference, *The Sedona Conference Glossary: E-Discovery & Digital Information Management (Fourth Edition)*, 15 SEDONA CONF. J. 339 (2014), https://thesedonaconference.org/publication/The_Sedona_Conference_Glossary.

¹²See Fed. R. Evid. 902 advisory committee’s note to 2017 amendment; see also *Gasperini*, 729 F. App'x at 114-15 (holding that the evidence was authentic, in part, because the copies of data were “validated by matching the ‘hash values’ of the copies and originals”).

¹³Both subsections 13 and 14 reference the notice requirements of Rule 902(11). It is from that rule that the quote above was taken.

¹⁴See Fed. R. Evid. 902 advisory committee’s note to 2017 amendment.

¹⁵In the criminal context, the government may also want to consider issues stemming from the Sixth Amendment’s right to confront witnesses.

¹⁶See *United States v. Zuschlag*, No. 2:16-CR-158, 2008 WL 2669957, at *4 (D. Me. June 4, 2018).

¹⁷*La Force v. GoSmith, Inc.*, No. 17-cv-05101, 2017 WL 9938681, at *3 (N.D. Cal. Dec. 12, 2017) (Plaintiff disputed that certain terms of use that defendant was citing as the basis for the agreement to arbitrate were in fact the terms plaintiff had agreed to at the time. The court disagreed, citing, in part, that the screenshots of previously used terms on the website were not properly authenticated.).