Follow the Audit Trail: The Impact of Metadata in Litigation

By: Mark D. Hansen and Tyler J. Pratt

Mark D. Hansen is a shareholder in the Peoria, Illinois office of Heyl, Royster, Voelker & Allen. He has extensive experience in complex litigation, with an emphasis in professional liability, business and commercial litigation, and product liability.

Tyler J. Pratt is a senior associate in the Champaign, Illinois office of Heyl, Royster, Voelker & Allen. He focuses his practice in the areas of professional liability, business and commercial litigation, and trucking litigation.

WITH the ever-changing world of technology and its permeation in nearly every aspect of life, the volume of electronic documents and data created on a daily basis is immense. In 2015, the number of emails sent and received per day supposedly totaled over two hundred five billion. That number is expected to grow at an average annual rate of three percent, reaching nearly two hundred forty-six billion by the end of 2019. The invention of smart phones and tablets have not only increased the number of emails, but caused the use of text messages, social media, and collaboration through cloud platforms such as Google Docs, to skyrocket. It is not surprising that this information is beneficial to litigators involved in business, commercial, personal injury, and family law areas, but the role of electronic devices, electronically stored information, and metadata have also become increasingly important in litigation, specifically medical malpractice, automobile and trucking, product liability, trademark cases and criminal prosecutions, to name a

few. Consequently, producing records solely from a paper file located on a shelf or filing cabinet is a relic of a bygone era and practitioners, regardless of their practice area, should make a conscious effort early in every case to determine whether discoverable electronic data and, particularly, metadata exist; assess whether it is relevant to the pertinent issues; and ensure its preservation.

I. What is Metadata?

Metadata is information that is not readily apparent from the face of an electronic document.[1] Metadata is commonly defined as "data about data."[2] "From a legal standpoint metadata is evidence … that describes the characteristics, origins, usage and validity of other electronic evidence."[3] There are two types of metadata: system metadata and application metadata.[4]

As the name implies, system metadata relates primarily to a computer's storage information. It is used to identify like where files are located on the hard drive, the file name, size, any modifications to the file, and usage.[5]

Alternatively, application metadata is located within the file itself.[6] Application metadata is oftentimes most useful to litigation because it can include information such as when a document was created, edited and/or accessed, the documents' author(s), and previous versions of the document.[7] For example, Microsoft Word documents contain metadata that "includes the author's name, the name of the computer used to create the file, the last time it was saved, the date it was created, and the creator's company name."[8] This type of data is embedded in the file and updated automatically.[9]

Documents created on computers are not the only medium in which metadata exists. Digital cameras, CDs, flash drives, and other mediums can also contain metadata. With respect to digital cameras, metadata can include the name of the manufacturer, lens setting, date the photos were taken, and lighting conditions. When the photo is uploaded, the computer will then create additional metadata regarding that photo. As for CDs and other mediums containing music, metadata can include the date of production, the artist, genre,

---

[1] Susan R. Gering, *Electronic Health Records: How to Avoid Digital Disaster*, 16 MICH. ST. U. J. MED. & L. 297, 306 (2012).
[2] Thomas R. McLean, *EMR Metadata Uses and E-Discovery*, 18 ANNALS OF HEALTH LAW 75, 75 (2009).
[3] Jeffrey L. Masor, *Electronic Medical Records and E-Discovery: With New Technology Come New Challenges*, 5 HASTINGS SCI. & TECH. L.J. 245, 252 (2013).
[4] *Id*.
[5] *Id.*
[6] *Id*.
[7] Gering, *supra* note 1, at 306.
[8] Masor, *supra* note 2, at 252.
[9] *Id*.

copyright, and owner. This type of data can be particularly useful in piracy prosecutions.

In sum, metadata is data that is automatically created and leaves snippets of information behind which can later reveal when an item was created, edited, revised, printed, accessed, tampered with, or produced. Now that we have a general understanding of what metadata is, we will explore some of the different areas of litigation where it can have an impact. Admittedly, the applications set forth below are limited in number because it can impact nearly every area of the law.

II. What Role Does Metadata Play in Litigation?

Without question, one of the most important roles metadata can play in litigation is its impact on the credibility of evidence—both oral testimony and documentary. As previously mentioned, metadata is typically created automatically and therefore in some respects can have the same effect as a videotape to show recorded activities. One example is where a physician testifies he created a note in the medical chart immediately after surgery, however, the relevant metadata suggests the medical record was not created until hours or days after the surgery. A one-time occurrence, especially if the note was created close in temporal proximity, is certainly a minor issue and could be easily explained away due to a faulty memory. However, the impact of metadata can present significant problems when it reveals habitual, fraudulent, or tampering activities. Conversely, metadata also has the reverse effect and can reinforce positive evidence, thus causing a party or witness to gain credibility with the fact finder. All things considered, while metadata can also be used circumstantially, at its core, even circumstantial evidence directly impacts credibility. Consequently, metadata's greatest role in litigation may be to test the veracity of an opponent's evidence and theory of the case.

III. Types of Metadata Available and Their Limitations

Almost any case can have metadata associated with email and Microsoft Office products such as Word, Excel, PowerPoint, etc. This is particularly true in business and commercial litigation. However, some cases are more unique and involve less common types of metadata. This section will explore some of those areas.

A. Medical Malpractice

In the area of medical malpractice, metadata is often created by audit control systems. These systems can show the use and access of a patient's records and the

operation of electronic devices that transmit or maintain records. [10] Typically, audit control systems are not part of a patient's medical records,[11] though these systems can provide a wealth of information that would otherwise be unobtainable through the discovery process. [12] The types of system metadata which may be available include audit trails, pop-ups, and preliminary questions and checkboxes that make up a finalized note.[13]

1. Audit Trail

"An audit trail is a record of who, when, where, how and sometimes why a person used a computer program or accessed a patient's medical record." [14] As discussed above, this can be useful in substantiating or invalidating witness testimony, such as the actions of physicians, nurses, or technicians, but it is not without its faults. In a rapidly changing environment, such as an emergency room, maintaining accuracy can be challenging. For instance, if a nurse administered medication at 7 a.m., but did not make the note until 7:30 a.m., the medical record would be time stamped 7:30 a.m. and would not be accurate. Similarly, if medical personnel are rapidly changing locations, mistakes can easily be made in the identification of treaters and services performed. While both issues can be easily remedied by timely charting and good practices, if a chart is littered with these types of inconsistencies, significant credibility concerns can arise and one must carefully analyze the circumstances surrounding the content of the metadata before taking it as the truth.

One such instance occurred in *Karam v. Adirondack Neurosurgical Specialists, P.C.*[15] There the plaintiff asserted defendants were negligent in failing to apprise the physician of changes in decedent's condition in a timely manner. The trial focused on the time at which decedent began to deteriorate neurologically. A note in decedent's emergency room record entered by Nurse Richard Dodge, reportedly at 11:23 a.m., stated that decedent was vomiting and starting to complain of a severe headache and that he was beginning to deteriorate in condition. That note described decedent's speech as "clear" and "[n]ormal," and his skin as "warm [and] dry," but the note also described his skin as "[m]oist [and] sweaty." Several witnesses testified for plaintiff that decedent began to deteriorate between 11:00 a.m. and 11:30 a.m. One witness

[10] James G. Meyer et al., *Electronic Medical Records: Metadata as Evidence in Litigation*, 101 ILL. B.J. 422 (2013).
[11] *Id*.
[12] *Id*.
[13] Masor, *supra* note 2, at 253.
[14] Meyer, *supra* note 10, at 422.
[15] 93 A.D.3d 1260, 941 N.Y.S.2d 402 (N.Y. Sup. Ct. App. Div. 2012).

testified that the hospital's computer system had been in place for only a few months at the time decedent was treated and that Dodge's note was inconsistent. He stated that it sometimes appeared "as if there were gremlins in [the] computer system." The witness further testified that it was possible that some of the entries for the 11:23 a.m. note had in fact been made at 12:35 p.m. Counsel for defendants admitted that, by procuring such witness testimony, he was impeaching in part defendants' own record. Counsel for defendants then attempted, though unsuccessfully, to introduce an "audit trail" of the computer system establishing that much of the 11:23 a.m. note was made at a later time. While it was not admitted due to defendants' failure to timely disclose the information, this case is a perfect illustration of not only how metadata can impact a case, but also some of the credibility concerns that can arise both from an evidentiary perspective.

2. Pop-Ups

Another control system is a "pop-up." A pop-up can be a warning, alert, or reminder that tells a physician about potential interactions between medications.[16] System metadata can show the EMR program warned the physician about the harmful interaction.[17] While this is not the be-all and end-all, it can be problematic if the nurse or physician are unable to set forth legitimate reasons for their actions or are unable to remember whether they received the pop-up message. The same can be applied to pharmaceutical cases.

3. Preliminary Questions and Checkboxes

Similar to pop-ups, preliminary questions and checkboxes contained in the records also contain metadata, and this metadata can substantiate or disprove a party's position.[18] These types of preliminary questions and checkboxes can establish whether the physician or nurse considered certain types of information and in some respects, acts as a reminder just like a pop-up. While these can be beneficial to prevent error, they can also be used to establish negligence if they go unanswered.

4. Conclusion

The take-away here is that while these programs are useful in minimizing mistakes, bad charting and inattention to detail can be easily revealed through metadata. Now more than ever, it is important for medical professionals to

[16] Masor, *supra* note 2, at 255.

[17] *Id*. at 256.

[18] *Id*.

carefully and timely chart patient records because metadata is making note of their every move.

B. Motor Vehicle and Trucking Litigation

Two of the most sensitive issues in motor vehicle and trucking accident litigation are the use of cell phones and electronic logging devices ("ELDs") (a/k/a driver log books). When combined with other electronic devices such as Event Data Recorders ("EDRs") and GPS navigation devices, electronic data can tell a different story of what occurred than that told by the involved drivers.

For example, imagine the benefit of being able to compare the metadata showing when text messages were sent or received on a smartphone to the EDRs vehicle data showing the driver's reactions times through braking, acceleration, and vehicle movement. Similar to computers, cell phone metadata is capable of showing the numbers dialed or texted, the length of calls, the location of the cell phone use, and the date and time of the calls, text messages, or internet use long after the user believes they have been deleted from the phone or their service provider has purged their records. Of course, the circumstances of the case will dictate whether obtaining this information is cost prohibitive. The same is true for ELDs.

ELDs have been implemented by numerous companies in an attempt to deter and reduce log book fraud, which in turn hopes to keep fatigued drivers off the road. An ELD synchronizes with a vehicle engine to automatically record driving time for easier, more accurate hours of service recording.[19] The implementation of ELDs will undoubtedly significantly reduce log book fraud, and any tampering will be exposed by the metadata created by the device.

C. Design Professional Litigation

Another example exists in the area of design professional litigation. Architects use a variety of software programs to assist in creating their blueprints and designs, most of which store metadata similar to the other computer programs identified above. Some of these programs also contain warnings that alert the user to items such as a deviation from the design criteria. This metadata can also be captured and utilized in litigation.

D. Other Areas

Metadata can be obtained in almost any case involving electronic devices. Some metadata may be

[19] https://www.fmcsa.dot.gov/hours-service/elds/electronic-logging-devices.

easier to obtain than others, but it should be readily apparent that it likely exists and can be applied in a similar manner to a multitude of areas of law. Those include, but certainly are not limited to the following practices:

- Patent and Trademark Law[20]
- Criminal Law
- Business and Commercial Law
- Aviation
- General Casualty/Tort
- Employment[21]
- Civil Rights[22]
- Governmental
- Product Liability[23]
- Pharmaceutical
- Workers' Compensation
- Professional Liability and Regulation/Licensure, and
- Securities Litigation.[24]

IV. Is Metadata Discoverable and Admissible?

Simply put, yes. Metadata is both discoverable and admissible. As one New York Court put it, "[w]hile certainly meta-data is discoverable to determine if and when documents may have been altered, that is not the only reason for production. General information about the creation of a document, including who authored a document and when it was created, is pedigree information often important for purposes of determining admissibility at trial."[25] With respect to discoverability, the issue will turn on relevance and proportionality. As for admissibility, the greatest challenges are accuracy and authenticity.

A. Discoverability of Metadata

The Federal Rules of Civil Procedure recognize the discoverability of metadata, as do many states.[26] By way of illustration, in Illinois Supreme Court Rule 201, the definition of "documents" includes "all retrievable information in computer storage."[27] Illinois Supreme Court Rule 214 further recognizes that the production includes "all retrievable information in computer storage."[28] Similarly, Federal Rule of Civil Procedure 34

[20] Celerity, Inc. v. Ultra Clean Holding, Inc., 476 F. Supp.2d 1159 (N.D. Cal. 2007).
[21] Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640 (D. Kan. 2005).
[22] Rodriguez v. City of Fresno, No. 1:05cv1017 OWW DLB, 2006 U.S. Dist. LEXIS 20125 (E.D. Cal. Apr. 7, 2006).
[23] *In re* Vioxx Prods. Liab. Litig., No. 1657, 2005 U.S. Dist. LEXIS 47306 (E.D. La. Feb. 17, 2005).
[24] *In re* Priceline.com Inc. Sec. Litig., 233 F.R.D. 88 (D. Conn. 2005).
[25] Hinshaw & Culbertson, LLP v. e-Smart Tech., Inc., 2012 NY Slip Op 30751(U), ¶ 5 (N.Y. Sup. Ct. March 26, 2012).
[26] ILL. SUP. CT., R 201 and 214; FED. R. CIV. PROC. 34.
[27] ILL. SUP. CT., R 201.
[28] ILL. SUP. CT. R 214.

also allows metadata to be discovered, though federal district courts have recognized that the request must specifically seek its production.[29] Regardless of where a case is venued, the real issues remain relevancy and proportionality. Once the requesting party shows the information is relevant, the burden shifts to the responding party to show an undue burden or expense.[30]

With respect to relevancy, metadata is generally treated just like any other document.[31] Metadata is relevant if the authenticity of a document is questioned or if establishing who received what information and when is important to the claims or defenses of a party.[32]

In other words, [i]n general, metadata is relevant when the process by which a document was created is in issue or there are questions concerning a document's authenticity; metadata may reveal when a document was created, how many times it was edited, when it was edited and the nature of the edits. In the absence of an issue concerning the authenticity of a document or the process by which it was created, most metadata has no evidentiary value.[33]

In applying the Sedona Principles, however, one bankruptcy court found it necessary to analyze relevancy based on the different categories of metadata.[34] The court recognized

> [t]here are three general categories or types of metadata, two of which are rarely discoverable. Substantive or

[29] Palar v. Blackhawk Bancorp., No. 11-4039, 2013 U.S. Dist. LEXIS 58082, at *4 (C.D. Ill. Mar. 19, 2013); Chapman v. General Bd. of Pension and Health Benefits of United Methodist Church Inc., No. 1:09-cv-03474, 2010 WL 2679961, 2010 U.S. Dist. LEXIS 66618 (N.D. Ill. July 6, 2010); *In re* Porsche Cars N. Am., Inc. Plastic Coolant Tubes Prods. Liab. Litig., 279 F.R.D. 447, 449 (S.D. Ohio 2012); Aguilar v. Immigration & Customs Enforcement Div. of U.S. Dep't of Homeland Sec., 255 F.R.D. 350, 355 (S.D.N.Y. 2006); Romero v. Allstate Ins. Co., 271 F.R.D. 96, 106 (E.D. Pa. 2010).

[30] Rawat v. Navistar Int'l Corp., No. 08 C 4305, 2011 U.S. Dist. LEXIS 98432, at *35-36 (N.D. Ill. Sep. 1, 2011), citing Susquehanna Comm. Finance, Inc. v. Vascular Resources, Inc., No. 1:09-CV-2012, 2010 U.S. Dist. LEXIS 127125, 2010 WL 4973317, at *13 (N.D. Ill. Dec. 1, 2010) ("courts have generally found that the burden rests with the party objecting to the production of metadata or ESI to show undue hardship or expense.").

[31] *Aguilar*, 255 F.R.D. at 355 (noting metadata is subject to FRCP 26 and 34).

[32] *Compare* Vargas v. Lee, 2015 NY Slip Op 31048(U) (N.Y. Sup. Ct. June 18, 2015) (considering authenticity) *with* Gilbert v. Highland Hosp., 31 N.Y.S.3d 397 (N.Y. Sup. Ct. 2016) (considering who received what information and when to claims and defenses).

[33] Kingsway Fin. Servs. v. Pricewaterhouse-coopers LLP, 2008 U.S. Dist. LEXIS 105222, at *18 (S.D.N.Y. Dec. 31, 2008), citing *Aguilar*, 255 F.R.D. at 353.

[34] Jemsek v. Jemsek Clinic, P.A. *(In re* Jemsek Clinic, P.A.*)*, Nos. 06-31766, 06-31986, 07-3006, 07-03008), 2013 Bankr. LEXIS 3120, at *26-27 (U.S. Bankr. W.D.N.C. Aug. 2, 2013).

> application metadata is embedded in the document and reflects substantive changes made by the user. Where available, substantive metadata may be useful to show prior editorial comments and information about fonts, spacing, etc. in the document. For example, this type of metadata will show how many words or characters are in a particular document. While relevant is some cases, the requesting party must show good cause to obtain production of substantive metadata. Similarly, system metadata is information created by the user or by an information technology system, such as author, date/time of creation, and date modified. Most courts have concluded that system and substantive metadata lack evidentiary value because they are rarely relevant to the merits of a parties' claim. In contrast, embedded metadata is not typically visible to a user but may be necessary to understand the document, such as Excel spreadsheet formulae or hyperlinks. This type of metadata is generally discoverable. (e.g., the native versions of Excel spreadsheets).[35]

Despite recognizing one discoverable type of metadata, the court still concluded that the metadata sought was irrelevant because the requesting party could not show the request was in good faith.[36] Similarly, it is insufficient to request metadata by simply asserting that the information "may provide discovery on the timing and substance of plaintiff's care."[37]

In contrast, appropriately defined requests are permissible. For example, in *Gilbert v. Highland Hospital*, Plaintiff sought discovery of the EMR audit trail to determine: (1) whether certain physicians were involved in her care and treatment and the extent, if any, of that involvement; (2) names and times of

---

[35] *Id.*

[36] *Id.*

[37] *Vargas*, 2015 NY Slip Op 31048(U), at ¶ 5; United Cent. Bank v. Kanan Fashions, Inc., No. 10 C 331, 2010 U.S. Dist. LEXIS 83700, at *6-7 (N.D. Ill. Aug. 12, 2010) (Defendants failed to articulate any particular need for metadata), citing *Kingsway Financial Serv., Inc.*, 2008 U.S. Dist. LEXIS 105222 at *6 ("[i]n light of the dubious value of metadata and plaintiffs' total failure to explain its relevance to the claims and defenses..., plaintiffs' application to compel its production is denied."); *Aguilar*, 255 F.R.D. at 355.

certain entries that were missing from the EMR; (3) the accuracy of the information in the EMR; and (4) the times, locations, and actions taken by various staff members not provided on the face of the EMR.[38] The court reasoned that since this information was important to the claims and defenses, the Plaintiff met the standard. Consequently, similar to any other document, in order to be relevant, the "information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence."[39]

As for proportionality, requests for metadata must comply with Federal Rules of Civil Procedure 26(b)(2) (C)(iii).[40] A party need not produce documents if "the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of discovery in resolving the issues."[41] A request for metadata is unduly burdensome where a party seeks duplicative document production in violation of Federal Rules of Civil Procedure 34(b)(2)(E)(iii).[42] But, if a requesting party satisfies the relevancy requirements and overcomes a responding party's proportionality argument, a court will likely require disclosure of the metadata.

B. Admissibility of Metadata

Two of the common hurdles encountered in admitting metadata involve authentication and hearsay.

1. Authentication

Under the Federal Rules, it may be necessary to retain an expert witness to authenticate metadata. This is particularly true if counsel believes the Court may be skeptical of such evidence, if questions arise regarding the chain of custody, or there is evidence that the data was manipulated or partially destroyed. It also could depend on the significance of the information to the case and whether the opposition will object. As a general rule, if one seeks to introduce metadata as evidence, the best practice is to retain an expert.

If the metadata relates to documents created in the ordinary course of business, self-authentication under Federal Rule of Evidence 902(11) could suffice.[43] It likely depends on the form in which it is produced and used, however, because if the documents

[38] *Gilbert*, 31 N.Y.S.3d 397.
[39] *Aguilar*, 255 F.R.D. at 355.
[40] *In re Jemsek Clinic, P.A.*, 2013 Bankr. LEXIS 3120, at *25.
[41] *Id.*
[42] *Id.* at *26.
[43] Rambus, Inc. v. Infineon Techs. AG, 348 F. Supp.2d 698 (E.D. Va. 2004); In the Interest of F.P., 2005 PA Super 220 (Pa. Sup. Ct. June 15, 2005).

are printed out, chances are that the metadata will contain strange symbols that are unintelligible to most individuals.[44] In those circumstances, self-authentication will be unavailable and expert testimony, or authentication through other measures, is likely necessary.[45]

Similarly, if system metadata must be authenticated, as opposed to application metadata, some combination of the following may be required: (1) a witness with knowledge; (2) an expert witness; (3) identification of distinctive characteristics; or (4) evidence that the system's output is known to be reliable, such as time-stamping of a computer record.[46]

Finally, under Federal Rule of Evidence 901(b)(9), evidence describing a process or system can be authenticated by producing evidence sufficient to support a finding that the item is what the proponent claims it is. One example is computer generated time stamps, which are mechanical traces that can be used to prove the occurrence of an event. [47] A time stamp is considered a "mechanical trace" for the purposes of admissibility.[48] This is critical because "[a] 'mechanical trace' [can be used] . . . to show that at some previous time a certain act was or was not done." [49] Just as importantly, absent proof of alteration, computer generated data, such as a time stamp attached to a file when it is saved, is generally admissible and taken as true. [50] While the authenticity of computer-generated data may be challenged if it has been altered, some evidence is required to justify excluding metadata.[51] Consequently, a stand-alone conclusory or speculative allegation that the metadata has been altered is insufficient and a party opposing computer generated data must put forth more than mere assertions of tampering.[52] "Absent

---

[44] McLean, *supra* note 2, at 79.

[45] Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 555 (D. Md. 2007) ("The most frequent ways to authenticate e-mail evidence are 901(b)(1) (person with personal knowledge), 901(b)(3) (expert testimony or comparison with authenticated exemplar), 901(b)(4) (distinctive characteristics, including circumstantial evidence), 902(7) (trade inscriptions), and 902(11) (certified copies of business record).").

[46] McLean, *supra* note 2, at 79.

[47] CA, Inc. v. Simple.com, Inc., 780 F. Supp.2d 196, 224-225 (E.D.N.Y. 2009).

[48] *Id*., citing L.A. News Serv. v. CBS Broad., Inc., 305 F.3d 924, 936 (9th Cir. 2002) (likening "a postmark or a time stamp" to a mechanical trace not subject to the hearsay rule because it is not an assertion).

[49] *CA, Inc.*, 780 F. Supp.2d at 224-225, quoting United States v. Snow, 517 F.2d 441, 443-444 (9th Cir. 1975) (citing WIGMORE §§ 25, 148-157 (3rd ed. 1940)).

[50] *CA, Inc.*, 780 F. Supp.2d at 224-225, citing 5-900 WEINSTEIN'S FEDERAL EVIDENCE § 900.07[1][a].

[51] *CA, Inc.*, 780 F. Supp.2d at 224, citing L.A. News Serv. v. CBS Broad., Inc., 305 F.3d 924, 936 (9th Cir. 2002) and *Snow*, 517 F.2d at 443-444.

[52] Floorgraphics, Inc. v. News Am. Mktg. In-Store Servs., 546 F. Supp.2d 155, 169 (D. N.J. Feb. 4, 2008) (noting that since there was not even a "shred" of evidence that the computer files were in any way manipulated,

specific evidence of tampering, allegations that computer data has been altered goes to its weight, not admissibility."[53]

As a general principle, there is no hard and fast rule when it comes to authenticating metadata. Instead, it is something that will be driven by the circumstances, the type of underlying data, and the source of the data and metadata. Consequently, extreme care must be exercised in order to ensure it is properly authenticated.

2. Hearsay

In an early decision on the issue, the Illinois Supreme Court held that metadata does not qualify as hearsay. In doing so, the Court has recognized the difference between computer generated information and information stored on a computer. [54] The Court held computer stored information may be hearsay, but computer generated information is not.[55] For example, the Court explained that a printout of results of computerized telephone tracing equipment was not hearsay evidence because "[t]he evidence is generated instantaneously as the telephone call is placed, without the assistance, observations, or reports from or by a human declarant. The printouts of such data are merely the tangible result of the computer's internal operations."[56] Illinois Appellate Courts have subsequently applied the same rationale to civil situations.[57]

Federal Courts have also applied a similar rationale and rule.[58] For example, in *CA, Inc. v. Simple.com, Inc.*, the New York Federal District Court noted that

> computer-generated data, which includes metadata, . . . are extrajudicial statements that are not hearsay. In these circumstances, there is no declarant making a statement. The computer is itself performing the transaction at issue. Thus, a hearsay foundation is unnecessary and the evidence can be admitted upon a proper

---

the proffered documents were reliable) (quoting United States v. Bonallo, 858 F.2d 1427, 1436 (9th Cir. 1988)); United States v. Steiger, 2006 U.S. Dist. LEXIS 89832, *68-69 (M.D. Ala. Sept. 7, 2006).

[53] *Steiger*, 2006 U.S. Dist. LEXIS 89832 at *68-69.

[54] People v. Holowko, 109 Ill.2d 187 (Ill. 1985).

[55] *Id*. at 191.

[56] *Id*.

[57] Aliano v. Sears, Roebuck & Co., 2015 IL App (1st) 143367 (Ill. App. Ct. December 30, 2015).

[58] 1st Fin. SD, LLC v. Lewis, No. 2:11-cv-00481-MMD-VCF, 2012 U.S. Dist. LEXIS 144334, at *6 (D. Nev. Oct. 5, 2012), citing *CA, Inc.*., 780 F. Supp.2d at 224 (E.D.N.Y. 2009); United States v. Khorozian, 333 F.3d 498, 505 (3d Cir. 2003).

> authentication foundation under Rule 901(b)(9).[59]

Similarly, in *United States v. Khorozian*, the Third Circuit held that a fax machine's automatically generated header was not hearsay because "nothing 'said' by a machine . . . is hearsay."),[60] and in *1st Fin. SD, LLC v. Lewis*, the Court denied defendant's motion *in limine* to exclude Microsoft Word documents that Plaintiffs planned to use to show the author of the documents. [61] In conclusion, assuming the metadata can be authenticated, it should not be excluded based solely on a hearsay objection.

V. Conclusion

Attorneys and their clients should be cognizant that any document created by electronic means can also leave a trail of potentially relevant admissible evidence that will test the veracity of the parties' allegations and evidence. This proverbial smoking gun has the potential to significantly impact any case. Metadata can contain a wealth of information and as long as practitioners learn of its existence and how to use it, benefits can be derived and damage can be mitigated. Don't be the one who is caught off guard and has to rely on the "computer 'Gremlins'" defense.[62]

---

[59] *CA, Inc.*, 780 F. Supp.2d at 224.

[60] *Khorozian*, 333 F.3d at 505, citing 4 MUELLER & KIRKPATRICK, FEDERAL EVIDENCE § 380, at 65 (2d ed.1994)).

[61] *1st Fin. SD*, 2012 U.S. Dist. LEXIS 144334, at *4.

[62] *Karam*, 93 A.D.3d at 1261 (inconsistencies within defendants' own medical record was impeached in part on emergency physician's testimony that the Hospital's computer system had been in place for only a few months at the time decedent was treated and that it sometimes appeared "as if there were gremlins in [the] computer system").