

THE NATURE AND SIGNIFICANCE OF METADATA

PHILIP J. FAVRO¹

The advent of electronically stored information has drastically changed the practice of law and presents daunting challenges for counsel and client alike. Of these challenges, perhaps none is more significant, yet less understood, than metadata. While often dismissed by the unwary as “digital clutter,” metadata is “the electronic equivalent of DNA, ballistics and fingerprint evidence, with a comparable power to exonerate and incriminate.”² Indeed, because metadata describes the characteristics, origin, and usage of electronically stored information and often cannot be discerned on the face of a document, it may have tremendous value or cause troublesome problems in a given case or transaction.³ The Federal Trade Commission’s inadvertent disclosure of Whole Foods’ trade secrets in court filings this month exemplifies the hazardous nature of metadata.⁴

Courts have recognized the significance of metadata, ordering its production on several occasions over the past two years.⁵ In addition, the 2006 amendments to the Federal Rules of Civil Procedure arguably impose a modest presumption in favor of preserving and producing relevant metadata.⁶ Given these developments, attorneys are now facing the reality of how to advise their clients to preserve such data and what measures they must take to obtain it from their counterparts. To do so, counsel must first understand what metadata is, as well as its potential magnitude in a case or transaction. This paper will address these issues. In particular, the paper will discuss the commonly used software applications that create files with metadata, describe the metadata in those file formats, and explore the drawbacks and benefits that metadata poses to attorneys and their clients.

¹ Senior Attorney, Packard, Packard & Johnson; J.D., Santa Clara University School of Law, 1999; B.A., Political Science, Brigham Young University, 1994. The author wishes to acknowledge that this paper was first published, in substantial part, by the Boston University Journal of Science & Technology Law in 2007 under the title *A New Frontier in Electronic Discovery: Preserving and Obtaining Metadata*.

² Craig Ball, *Understanding Metadata: Knowing Metadata’s Different Forms and Evidentiary Significance is Now an Essential Skill for Litigators*, 13 LAW TECH. NEWS, Jan. 2006, 36, 36.

³ *Id.*

⁴ Christopher S. Rugaber, *Error by FTC Reveals Whole Foods’ Trade Secrets*, WASHINGTON POST, August 15, 2007, at D03, available at http://www.washingtonpost.com/wp-dyn/content/article/2007/08/14/AR2007081401784_pf.html; see also Adam Liptak, *Prosecutors Can’t Keep a Secret in Case on Steroid Use*, N.Y. TIMES, June 23, 2006, at A18, available at <http://www.nytimes.com/2006/06/22/washington/22cnd-leak.html>.

⁵ *Celerity, Inc. v. Ultra Clean Holding, Inc.*, 476 F.Supp.2d 1159, 1164 (N.D. Cal. 2007); *G.D., D.D., E.P., P.P., J.O. and S.K. v. Monarch Plastic Surgery*, No. 06-2184-CM, slip op. at 8 (D. Kan. Jan. 24, 2007), available at 2007 WL 201154; *In re NYSE Specialists Sec. Litig.*, No. 03 Civ. 8264(RWS), 2006 WL 1704447, at *1 (S.D.N.Y. June 14, 2006); *Rodriguez v. City of Fresno*, No. 1:05cv1017 OWW DLB, 2006 WL 903675, at *3 (E.D. Cal. Apr. 7, 2006); *Hagenbuch v. 3B6 Sistemi Elettronici Industriali S.R.L.*, No. 04 C 3109, 2006 WL 665005, at *2 (N.D. Ill. Mar. 8, 2006); *In re Priceline.com Inc. Sec. Litig.*, 233 F.R.D. 88, 91 (D. Conn. 2005); *Nova Measuring Instruments Ltd. v. Nanometrics, Inc.*, 417 F. Supp. 2d 1121, 1122 (N.D. Cal. 2006); *CP Solutions PTE, Ltd. v. General Elec. Co.*, No. 3:04cv2150 (JBA)(WIG), slip op. at 9-12 (D. Conn. Feb. 6, 2006), available at 2006 WL 1272615; *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640, 650 (D. Kan. 2005); *In re Verisign, Inc. Sec. Litig.*, No. C 02-02270 JW, 2004 WL 2445243, at *1-2 (N.D. Cal. Mar. 10, 2006).

⁶ See Philip J. Favro, *A New Frontier in Electronic Discovery: Preserving and Obtaining Metadata*, 13 B.U. J. Sci. & TECH. L. 1, 18-21 (2007).

A. Electronic Documents Containing Metadata

As previously mentioned, metadata is digitally stored information about a document's characteristics, including its origin and usage.⁷ Metadata is best characterized and understood, however, by moving beyond the abstract and examining the software applications that commonly utilize metadata. Those applications of most concern to attorneys and their clients typically include Microsoft Word, Adobe Portable Document Format ("PDF"), e-mail, Microsoft Excel and Corel Word Perfect.

I. Metadata in Microsoft Word

Microsoft Word documents contain metadata that can be both helpful and harmful to a user.⁸ The most commonly found metadata in Word documents includes the document author, the date the document was created, the identities of the last ten persons who edited the document, the dates when the revisions occurred, the text that was revised, tracked changes in the document, the location on the particular device where the document was stored, and various other fundamental traits concerning the document.⁹ Of these features, the "track changes" function is perhaps the most significant.¹⁰

Most attorneys are familiar with the "track changes" tool because it allows them to show changes to previous drafts of a document, along with the identities of document editors and the dates edits were made. These features make the track changes function a valuable tool for both attorney and client by allowing both parties to view and understand the evolution of a document.¹¹ However, such transparency is precisely what makes the track changes feature so problematic.¹² Unless the user specifically turns off the track changes function, changes made to the document and other pertinent information could be accessed by opposing counsel if the document is served in Word format.¹³ Indeed, imagine a defendant serving a plaintiff with a version of its written interrogatory responses that describe defenses to the plaintiff's claims. The defendant's lead counsel would have finalized the responses only after exchanging several drafts with her colleagues and client. Those exchanges contained notes in the responses from both counsel and client, including a potential discussion of the relative strength of each asserted defense. Unless defendant's counsel turned off the track changes feature or otherwise took measures to remove or "scrub" the metadata from the responses, plaintiff's counsel can exploit this mistake and explore the evolution of the responses, along with the confidential exchanges between attorney and client.¹⁴

If this scenario isn't troubling enough, the "track changes" feature also potentially permits a user to view the text of an unrelated document that the author used as a template for the current file.¹⁵ The practice of using an unrelated document as a template, common among lawyers due to its efficiency, can present a myriad of practical and ethical problems unless properly handled.¹⁶

⁷ Ball, *supra* note 2, at 36 (noting that metadata "sheds light on the context, authenticity, reliability and dissemination of electronic evidence, as well as providing clues to human behavior").

⁸ See Donna Payne, *Metadata - Are you Protected?* 1, http://www.payneconsulting.com/pub_books/articles/pdf/MidwestBarAssociationConferenceMetadataHandout.pdf (last visited July 30, 2007) [hereinafter Payne, *Metadata - Are you Protected?*]; Donna Payne, *Metadata: the Good, the Bad, and the Ugly: What it Means to Law Firms*, LAW OFFICE COMPUTING, Feb./Mar. 2004, at 78, 80-82, available at <http://www.payneconsulting.com> (follow "publication/books" hyperlink - requires registration) [hereinafter Payne, *Metadata: the Good, the Bad, and the Ugly*].

⁹ *Id.* at 80; see also J. Brian Beckham, *Production, Preservation, and Disclosure of Metadata*, 7 COLUM. SCI. & TECH. L. REV. 1, 2-3 (2006) (listing various metadata in Word documents). Donna Payne from the Payne Consulting Group indicates that additional Microsoft Word metadata includes the following: "Attached template," "Category, keywords and comments," "Company name," "Custom Properties such as client and matter or docID," "Embedded objects," "Graphics and more," "Hidden text," "Manager," "Routing slip," "Subject," "Title" and "Versions." Payne, *Metadata: the Good, the Bad, and the Ugly*, *supra* note 7, at 80.

¹⁰ See Tom Zeller, Jr., *Link by Link: Beware Your Trail of Digital Fingerprints*, N.Y. TIMES, Nov. 7, 2005, at C5, available at <http://www.nytimes.com/2005/11/07/business/07link.html?ex=1170824400&en=d01167df039d93d9&ei=5070>; Stephen Shankland, *Hidden Text Shows SCO Prepped Lawsuit Against BofA*, CNET NEWS.COM, Mar. 4, 2004, http://news.com.com/Hidden+text+shows+SCO+prepped+lawsuit+against+BofA/2100-7344_3-5170073.html.

¹¹ See *In re* 3817 W. West End, First Floor Chicago, Ill. 60621, 321 F. Supp. 2d 953, 956 n.1 (N.D. Ill. 2004) (explaining that metadata could show "not only the date a document was last saved, but also when the document was first created and (often times) the changes in the documents from the original draft to the final revision.").

¹² See Shankland, *supra* note 9.

¹³ *Id.*

¹⁴ See, e.g., Payne, *Metadata - Are you Protected?*, *supra* note 7, at 3; Payne, *Metadata: the Good, the Bad, and the Ugly*, *supra* note 7, at 80, 82; Beckham, *supra* note 8, at 2. That this scenario presents ethical implications for counsel has not gone unnoticed. The New York State Bar Association has issued opinions proscribing counsel from accessing metadata in electronic documents received from their counterparts. See Jessica M. Walker, *What's a Little Metadata Mining Between Colleagues?*, LAW.COM LEGAL TECHNOLOGY, Apr. 21, 2006, <http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1145538533635>. In sharp contrast to the New York Bar, the American Bar Association issued an Ethics Opinion on November 9, 2006, that may give attorneys free reign to harvest metadata from their counterparts. According to an ABA news release regarding the new ethics opinion: "Lawyers who receive electronic documents are free to look for and use information hidden in metadata . . . even if the documents were provided by an opposing attorney." *Lawyers Receiving Electronic Documents Are Free to Examine 'Hidden' Metadata: ABA Ethics Opinion*, November 9, 2006, http://www.abanet.org/abanet/media/release/news_release.cfm?releaseid=48.

¹⁵ Payne, *Metadata: the Good, the Bad, and the Ugly*, *supra* note 7, at 80.

¹⁶ See Walker, *supra* note 13; *The Sedona Principles, Second Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Discovery* 60 (The Sedona Conference Working Group Series, 2007) [hereinafter *The Sedona Principles*]. Irrespective of the ethical implications, counsel must take heed to protect against inadvertently divulging metadata, as some courts may determine that such a disclosure waives any protection afforded by the attorney-client privilege or work product doctrine. See *Hopson v. Mayor and City Council of Baltimore*, 232 F.R.D. 228, 236-38 (D. Md. 2005) (reviewing prior cases and concluding that the Fourth Circuit takes a "very strict interpretation of the attorney-client privilege" and "an unforgiving view of the results of its waiver").

2. Metadata in Adobe PDF Files

Many attorneys believe the solution to these problems is to simply convert a document from Word format into an Adobe PDF file.¹⁷ This practice is common among law firms, which often post documents to their websites in PDF and have been led to believe that PDF is a “static” format that contains no metadata.¹⁸ While its contents may or may not be altered, a PDF can still contain metadata.¹⁹ For example, unless appropriate precautions are taken, PDF metadata may include data imported from the original Word document.²⁰ This could include all of the “comments and tracked changes if they are contained in the original document.”²¹ PDF files also contain information about the file author, the date the file was created and modified, and a summary of the document.²²

3. Metadata in E-Mail, Excel, and Word Perfect

Other commonly used software applications replete with metadata include e-mail applications, Excel, and Word Perfect. E-mail metadata has “the same types of identifying data as do other electronic documents.”²³ It also includes data that may be viewable to all users, such as internet protocol addresses, the dates the e-mail was sent, received, replied to, and forwarded, and data that may not be readily accessible to certain viewers, such as blind carbon copy (“bcc”) information and sender address book data.²⁴

As a Microsoft application, Excel contains much of the same metadata found in Word, including author and revision history information.²⁵ It also contains “calculations that are not visible in a printed version or completely hidden columns that can only be viewed by accessing the spreadsheet in its ‘native’ application.”²⁶

Word Perfect contains some of the same strains of metadata found in Word.²⁷ In addition, Word Perfect has a unique feature known as the “Undo/Redo History.” This feature allows the author--and, unless appropriate care is taken, any recipient of the document--to access the last 300 actions taken in that particular file.²⁸ If, as mentioned in the previous hypothetical, defendant’s counsel served interrogatory responses in Word Perfect with the Undo/Redo History intact, opposing counsel could delve into much of the same historical information about the responses which would be accessible through Word’s track changes tool.²⁹

¹⁷ Payne, *Metadata – Are you Protected?*, supra note 7, at 2; Payne, *Metadata: the Good, the Bad, and the Ugly*, supra note 7, at 83.

¹⁸ Payne, *Metadata – Are you Protected?*, supra note 7, at 2; Payne, *Metadata: the Good, the Bad, and the Ugly*, supra note 7, at 83.

¹⁹ Payne, *Metadata – Are you Protected?*, supra note 7, at 2; Payne, *Metadata: the Good, the Bad, and the Ugly*, supra note 7, at 83; Applied Discovery, *File Formats for Electronic Document Review: Why PDF Trumps TIFF*, at 3, http://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_PDF_TrumpsTIFF.pdf (last visited July 30, 2007).

²⁰ Applied Discovery, supra note 18, at 3.

²¹ See Payne, *Metadata: the Good, the Bad, and the Ugly*, supra note 7, at 83.

²² *Id.*

²³ Beckham, supra note 8, at 4.

²⁴ *Armstrong v. Executive Office of the President*, 1 F.3d 1274, 1280, 1284 (D.C. Cir. 1993) (“important information present in the e-mail system, such as who sent a document, who received it, and when that person received it, will not always appear on the computer screen and so will not be preserved on the paper print-out”); Sharon Nelson and John Simek, *Metadata: What You Can’t See Can Hurt You*, 32 No. 2 LAW PRACT. 28, 29 (Mar 2006); *The Sedona Principles*, supra note 15.

²⁵ Microsoft, *How to Minimize Metadata in Microsoft Excel Workbooks*, <http://support.microsoft.com/kb/223789/en-us> (last visited July 30, 2007).

²⁶ *The Sedona Principles*, supra note 15, at 4; see also *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640, 647 (D. Kan. 2005).

²⁷ Payne, *Metadata – Are you Protected?*, supra note 7, at 2; Payne, *Metadata: the Good, the Bad, and the Ugly*, supra note 7, at 79-80.

²⁸ Payne, *Metadata: the Good, the Bad, and the Ugly*, supra note 7, at 79; see also Dan Pinnington, *Beware the Dangers of Metadata*, LAWPRO MAG., June 2004, at 36, 37, available at <http://www.practicepro.ca/LawPROmag/metadata.pdf>.

²⁹ See Pinnington, supra note 27, at 36-37.

B. Dealing with the Hazards of Metadata

As many attorneys and their clients know, the danger of disclosing metadata is not merely hypothetical.³⁰ When the SCO Group filed suit against DaimlerChrysler in 2004 for licensing violations related to an earlier version of IBM's open-source UNIX code, an electronic version of the complaint showed that SCO was planning to sue Bank of America instead of Chrysler.³¹ The "track changes" feature in Word allowed third parties to uncover this work product, including the date and time when SCO abandoned its efforts to sue Bank of America.³² That sophisticated technology companies have inadvertently disclosed attorney work product further underscores the importance of understanding and addressing the dangers of metadata.³³

Despite its troublesome nature, metadata can often be managed with appropriate precautions.³⁴ Typically, metadata will only be disclosed to opposing counsel and others through electronic sharing of files by sending e-mail attachments or sharing media such as flash drives, CD-ROMs, DVD-ROMs, or floppy disks.³⁵ Accordingly, counsel may control the flow of metadata by monitoring and controlling the materials that leave the office.³⁶ One means of doing so is to purchase software that will "scrub" the metadata from e-mail attachments before the information is exposed to opposing counsel and others.³⁷ In addition, before serving pleadings, discovery responses, and the like, those materials may be converted to Tagged Image File Format ("TIFF") documents, which have no metadata.³⁸ Electronic discovery consultants may also be retained to advise how to recognize problematic metadata and to assist in removing it from electronic documents.³⁹ Like most difficulties in the practice of law, the problem of metadata is not intractable and can be managed with appropriate care.⁴⁰

³⁰ See Shankland, *supra* note 9.

³¹ *Id.*

³² *Id.*

³³ While some may have viewed this disclosure as a tactical maneuver by SCO, it could just as easily have been a mistake by SCO's legal counsel. Beckham, *supra* note 8, at 3.

³⁴ Pinnington, *supra* note 27, at 37; Payne, *Metadata - Are you Protected?*, *supra* note 7, at 3-4.

³⁵ See Pinnington, *supra* note 27, at 37.

³⁶ See *id.*

³⁷ Various vendors, including the Payne Consulting Group, offer a number of these products for sale. See *id.*

³⁸ See Applied Discovery, *supra* note 18.

³⁹ Absent court approval or agreement from opposing counsel, "scrubbing" or otherwise impairing a document's metadata may run afoul of a party's discovery obligations. See FED. R. CIV. P. 34 advisory committee's note, 2006 Amendment to subdivision (b) ("If the responding party ordinarily maintains the information it is producing in a way that makes it searchable by electronic means, the information should not be produced in a form that removes or significantly degrades this feature."); Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 656 (D. Kan. 2005) (holding that defendant's removal of metadata from certain spreadsheets it produced in discovery was improper).

⁴⁰ Pinnington, *supra* note 27, at 37; Payne, *supra* note 7, at 3-4.

C. The Value of Metadata

Once appropriate steps are taken to control the hazards of metadata, its value may be realized.⁴¹ One of the significant benefits of metadata is its usefulness in authenticating documents.⁴² Because the inherent traits of metadata may enable a party to establish such things as when a document was created, the identity of the person who prepared the document, the purpose for doing so, and where the document was subsequently maintained, a party can more easily meet the authentication requirements under the Federal Rules of Evidence and applicable state law.⁴³ Such information may likewise be invaluable in a trade secret action because the issues in such cases typically focus on the “who,” “what,” “when,” and “how” inquiries surrounding removal of a party’s proprietary materials.⁴⁴

Metadata also performs a crucial function in establishing whether a document is genuine. The basic metadata characteristics described above can show whether a document has been inadvertently or intentionally modified.⁴⁵ Indeed, most court decisions addressing the significance of metadata have recognized its value in demonstrating document integrity.⁴⁶ The inherent traits of metadata also make it an effective document management device⁴⁷ and “useful for system administration as it reflects data regarding the generation, handling, transfer, and storage of the document or file within the computer system.”⁴⁸

Metadata can also function as a security device that companies may employ to protect privileged communications, work product, or proprietary interests contained in certain records.⁴⁹ For example, when a telecommunications company sent a highly confidential and privileged litigation hold instruction to its employees by e-mail, it attached an “electronic tracer” to the e-mail which allowed the company to monitor whether the message was forwarded outside the company.⁵⁰ This technique allowed the company to manage the flow of privileged information and ascertain the loyalty of its employees.⁵¹

⁴¹ See Ball, *supra* note 2, at 36.

⁴² See Lorraine v. Markel American Ins. Co., 241 F.R.D. 534, 547-548 (D. Md. 2007) (“Because metadata shows the date, time and identity of the creator of an electronic record, as well as all changes made to it, metadata is a distinctive characteristic of all electronic evidence that can be used to authenticate it under [Federal Rule of Evidence] 901(b)(4).”)

⁴³ *Id.*; *The Sedona Principles*, *supra* note 15, at 4, 61, 63; see also, e.g., FED. R. EVID. 901; CAL. EVID. CODE §§ 1400-1402 (West 2006).

⁴⁴ See *The Sedona Principles*, *supra* note 15, at 4.

⁴⁵ *Id.* at 46; Plasse v. Tyco Electronics Corp., 448 F.Supp.2d 302 (D. Mass. 2006) (dismissing lawsuit after analyzing metadata that revealed plaintiff had fabricated and deleted key evidence from his computer); PML North America, LLC v. Hartford Underwriters Ins. Co., No. 05-CV-70404-DT, slip op. at 5 (E.D. Mich. Dec. 20, 2006), *available at* 2006 WL 3759914 (finding that metadata established “evidence destruction” had transpired); see also, *Munshani v. Signal Lake Venture Fund II, LP*, No. 005529BLS, 2001 WL 1526954, at *2 (Mass. Super. Ct. Oct. 9, 2001) (dismissing lawsuit due to plaintiff’s fabrication of e-mail), *aff’d*, 60 Mass. App. Ct. 714 (2004); *Covucci v. Keane Consulting Group, Inc.*, No. 033584, 2006 WL 2004215, at *1, *8-9 (Mass. Super. Ct. May 31, 2006) (dismissing plaintiff’s lawsuit due to fabrication and destruction of evidence).

⁴⁶ See *Wild v. Alster*, 377 F. Supp. 2d 186, 194-195 (D.D.C. 2005) (denying motion for new trial where photographs would not have established malpractice since metadata showed the dates when photographs were imported onto a computer and not the dates the photographs were taken); *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640, 647 (D. Kan. 2005); *In re 3817 W. West End, First Floor Chicago, Ill.* 60621, 321 F. Supp. 2d 953, 956 n.1 (N.D. Ill. 2004); *Momah v. Albert Einstein Medical Center*, 164 F.R.D. 412, 418 (E.D. Pa. 1996) (ordering production of electronic file where the file’s metadata was potentially relevant to establishing plaintiff’s wrongful termination claim); *Armstrong v. Executive Office of the President*, 1 F.3d 1274, 1280, 1284-85 (D.C. Cir. 1993); *In re Genetically Modified Rice Litigation*, No. 4:06 MD 1811 CDP, slip op. at 5 (E.D. Mo. June 5, 2007), *available at* 2007 WL 1655757 (issuing preservation order requiring that for all custodians “a complete backup” be made of “all Active Files . . . without altering metadata”); *Krumwiede v. Brighton Assoc.*, No. 05 C 3003, slip op. at 20-21 (N.D. Ill. May 8, 2006), *available at* 2006 WL 1308629 (holding that a sanction of default judgment was appropriate since the plaintiff’s removal of metadata compromised the genuineness of the documents and foreclosed the defendant from proving its counterclaims); *Rodriguez v. City of Fresno*, No. 1:05cv1017 OWW DLB, 2006 WL 903675, at *3 (E.D. Cal. Apr. 7, 2006) (ordering defendants to produce metadata corresponding to certain police reports so the plaintiffs could determine the nature of any changes made to those documents); *Hagenbuch v. 3B6 Sistemi Elettronici Industriali S.R.L.*, No. 04 C 3109, 2006 WL 665005, at *2-3 (N.D. Ill. Mar. 8, 2006) (holding that removal of metadata from documents was inappropriate); *CP Solutions PTE, Ltd. v. General Elec. Co.*, No. 3:04cv2150 (JBA)(WIG), 2006 WL 1272615, at *10-11 (D. Conn. Feb. 2, 2006) (ordering defendant to produce metadata that would allow the plaintiff to link up e-mails produced by the defendant with their respective attachments); *In re Telxon Corp. Sec. Litig.*, No. 5:98CV2876, 1:01CV1078, 2004 WL 3192729, at *22, *34 (N.D. Ohio July 16, 2004) (entering default judgment against defendant after analysis of metadata demonstrated defendant modified its records in violation of court directives).

⁴⁷ Pinnington, *supra* note 27, at 36.

⁴⁸ *The Sedona Principles*, *supra* note 15, at 3.

⁴⁹ See *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age* 80 (The Sedona Conference Working Group Series, Sept. 2005) (“Individuals who create and transmit electronic documents are often unaware of the existence of readable metadata that may inadvertently reveal privileged or confidential information to adversaries and other outside parties.”).

⁵⁰ *Toftely v. Qwest Communications Corp.*, No. C3-02-1474, 2003 WL 1908022, at *1 (Minn. App. Apr. 22, 2003) (denying plaintiff employment benefits because she was discharged for violating the company’s confidentiality policy by disclosing litigation hold instruction to a third party).

⁵¹ *Id.*

D. Understanding Metadata Enhances Effective Client Representation

Metadata constitutes a significant aspect of almost all digital information, particularly in files generated by computer software applications that are used every day by lawyers and clients. When metadata is unknown, ignored or not properly controlled, counsel and client may encounter problems they could have otherwise avoided. However, when properly understood and utilized, metadata can provide tremendous value for companies in their respective fields and an enormous advantage for attorneys in litigation.⁵²

⁵² See *Hannan v. Dusch*, 154 Va. 356, 379 (1931) (“The law helps those that help themselves, generally aids the vigilant, but rarely the sleeping, and never the acquiescent.”)