

# ARTICLE

## A NEW FRONTIER IN ELECTRONIC DISCOVERY: PRESERVING AND OBTAINING METADATA

PHILIP J. FAVRO\*

### TABLE OF CONTENTS

I.	INTRODUCTION .....	
II.	THE NATURE AND SIGNIFICANCE OF METADATA.....	
	A. <i>Electronic Documents Containing Metadata</i> .....	
	1. Metadata in Microsoft Word .....	
	2. Metadata in Adobe PDF Files .....	
	3. Metadata in E-Mail, Excel, and Word Perfect.....	
	B. <i>Dealing with the Hazards of Metadata</i> .....	
	C. <i>The Value of Metadata</i> .....	
	D. <i>Understanding Metadata Enhances Effective Client     Representation</i> .....	
III.	RECENT CASE LAW DEVELOPMENTS ON PRODUCTION OF METADATA.....	
	A. <i>Notable Pre-2006 Case Law – Armstrong, Telxon and     Williams</i> .....	
	B. <i>Significant 2006 Case Law – Hagenbuch and Krumwiede</i> .....	
	C. <i>The Continued Viability of Metadata Case Law Is Largely     Dependant on the Newly Amended Federal Rules of Civil     Procedure</i> .....	
IV.	AMENDMENTS TO THE FEDERAL RULES OF CIVIL PROCEDURE AND THEIR IMPACT ON METADATA PRESERVATION AND PRODUCTION .....	
	A. <i>Amendments to Rules 16, 26(A) and 26(F) – Addressing     Metadata Issues Early in the Litigation</i> .....	
	B. <i>Amendments to Rule 34 – Implied Right to Obtain Relevant     Metadata</i> .....	
	C. <i>New Rule 37(F) – Safe Harbor against Sanctions for     Metadata Spoliation</i> .....	
	D. <i>The Amended Rules Appear Consistent With Case Law     Addressing Metadata Production and Preservation</i> .....	
V.	SUGGESTED PRACTICES FOR METADATA PRESERVATION AND PRODUCTION .....	
	A. <i>Implement a Timely Litigation Hold</i> .....	
	B. <i>Check the Local Rules</i> .....	
	C. <i>Determine and Specify the Form of Production</i> .....	

---

\* Senior Attorney, Packard, Packard & Johnson; J.D., Santa Clara University School of Law, 1999; B.A., Political Science, Brigham Young University, 1994.

D. Specifically Request “Electronically Stored Information” .....  
E. Clarify Whether Court Orders Require Metadata Disclosure.....  
VI. CONCLUSION .....

The digital age and its accompanying technological innovations have significantly changed the practice of law. Most information is now stored in electronic form rather than paper, and a host of new challenges confront attorneys and their clients which did not exist just a few years ago. One of those challenges is preserving and producing the embedded text found in electronic documents commonly referred to as metadata. Several courts have recently ordered production of metadata, and 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. This article will discuss the nature and value of metadata and the impact of case law and recent amendments to the Federal Rules of Civil Procedure on the preservation and production of metadata. It will also suggest some practice tips regarding metadata preservation and production.

## I. INTRODUCTION

The world has undergone a dramatic transformation with the arrival of the digital age. Whereas the business world used to be driven by paper transactions, many companies are now striving to move toward paperless operations. Gradually introduced into the business world during the 1980s, computers were so thoroughly integrated into society during the 1990s that in 1999, approximately 93% of all information created in that year was done so electronically.<sup>1</sup> This trend is likely to continue.<sup>2</sup>

Perhaps nowhere has this transformation been felt more acutely than in the legal profession. Less than ten years ago, many lawyers exchanged offers with paper, sent only hard copy letters (with the occasional facsimile), and filed “paper” at court. With the advent of the digital age, lawyers have been forced to adopt and adapt technologies that have significantly altered basic aspects of the practice of law.

---

<sup>1</sup> Kenneth J. Withers, *Electronic Discovery: The Challenges and Opportunities of Electronic Evidence*, Address at the National Workshop for Magistrate Judges (July 2001) (“According to a University of California study, 93% of all information generated during 1999 was generated in digital form, on computers. Only 7% of information originated in other media, such as paper.”), *quoted in In re Bristol-Myers Squibb Sec. Litig.*, 205 F.R.D. 437, 440 n.2 (D.N.J. 2002).

<sup>2</sup> See Donna Payne, *Metadata – Are you Protected?* 1, [http://www.payneconsulting.com/pub\\_books/articles/pdf/MidwestBarAssociationConferenceMetadataHandout.pdf](http://www.payneconsulting.com/pub_books/articles/pdf/MidwestBarAssociationConferenceMetadataHandout.pdf) (last visited Aug. 24, 2006) [hereinafter Payne, *Metadata – Are you Protected?*].

Take, for example, the litigator who represents a company's business interests in litigation. Prior to the digital age, such a lawyer would characteristically request and receive paper copies of contracts, correspondence, and other materials during discovery to evaluate and resolve typical business disputes for her clients. It was only the exceptional suit that would involve electronic evidence.<sup>3</sup>

Contrast that scenario with a litigator in the digital age representing the same company. Among other things, counsel must sort through various electronic drafts and versions of the contract and other materials, cull through thousands of e-mails, and work with clients and colleagues to ensure none of this information is altered, modified or destroyed.<sup>4</sup>

Though the legal landscape has unquestionably changed, the overall purposes of discovery remain the same: to "narrow and clarify" the issues in dispute,<sup>5</sup> and to "make a trial less a game of blind man's buff and more a fair contest with the basic issues and facts disclosed to the fullest practicable extent."<sup>6</sup>

To meet these objectives in the digital age, the "digital litigator" must adopt new rules of engagement to effectively represent her clients. One such "rule" is that an attorney should seek electronic files instead of settling for paper documents. In the electronic age, it is not a question of *whether* electronic data should be produced,<sup>7</sup> but what *form* the production should take.<sup>8</sup> Indeed,

---

<sup>3</sup> See, e.g., *In re Air Disaster at Detroit Metro. Airport*, 130 F.R.D. 634, 636 (E.D. Mich.1989) (ordering production of electronic data since earlier paper productions did not sufficiently encompass the sought after evidence); *Daewoo Elec. Co. v. United States*, 10 Ct. Int'l Trade 754, 757 (1986) (ordering production of defendant's computer tapes and all other forms of storage for electronic data); *Williams v. Owens-Illinois, Inc.*, 665 F.2d 918, 933 (9th Cir. 1982) (declining to order production of computer tapes where previously produced wage cards included sought after information); *Nat'l Union Elec. Corp. v. Matsushita Elec. Indus. Co.*, 494 F. Supp. 1257, 1258, 1263 (E.D. Pa. 1980) (ordering plaintiff to create computer readable tape containing certain data previously supplied to defendants in paper).

<sup>4</sup> See *Zubulake v. UBS Warburg LLC (Zubulake V)*, 229 F.R.D. 422, 431-434 (S.D.N.Y. 2004) (detailing counsel's obligations to ensure client compliance with litigation hold instructions and observance of its duty to preserve evidence).

<sup>5</sup> *Hickman v. Taylor*, 329 U.S. 495, 501 (1947).

<sup>6</sup> *United States v. Procter & Gamble Co.*, 356 U.S. 677, 682 (1958).

<sup>7</sup> See, e.g., FED. R. CIV. P. 34 advisory committee's note, 1970 Amendment to subdivision (a) ("Rule 34 applies to electronic data compilations from which information can be obtained only with the use of detection devices . . ."); *Rowe Entm't, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421, 428 (S.D.N.Y. 2002) ("Electronic documents are no less subject to disclosure than paper records."); *Simon Prop. Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639, 640 (S.D. Ind. 2000) ("[C]omputer records . . . are documents discoverable under Fed. R. Civ. P. 34."); *Playboy Enter., Inc. v. Welles*, 60 F. Supp. 2d 1050, 1053 (S.D.

disputes now abound concerning the appropriate form for electronic document production.<sup>9</sup>

In addition to questions regarding the form of production, a significant developing issue is whether parties have an obligation to preserve and produce an electronic document's metadata. Metadata, typically characterized as "data about data," is electronically stored detail about, among other things, the "characteristics, origin, usage and validity" of electronic data.<sup>10</sup> A reader often cannot view that information on a paper print-out of a document<sup>11</sup> or while editing the document in electronic format.<sup>12</sup> Such information is not "invisible" to everyone, however; metadata can be accessed by the computer savvy or may inadvertently become viewable. This characteristic is precisely

---

Cal. 1999) ("The Advisory Committee Notes to Fed. R. Civ. P. 34 referenced above makes [sic] it clear that information stored in computer format is discoverable."); *Anti-Monopoly, Inc. v. Hasbro, Inc.*, No. 94CIV.2120(LMM)(AJP), 1995 WL 649934, at \*2 (S.D.N.Y. Nov. 3, 1995) ("[T]oday it is black letter law that computerized data is discoverable if relevant.").

<sup>8</sup> See, e.g., *Rodriguez v. City of Fresno*, No. 1:05cv1017 OWW DLB, 2006 WL 903675, at \*3 (E.D. Cal. Apr. 7, 2006) (ordering production in electronic format instead of paper copies); *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) (ordering defendant to produce all electronic media in native format since that was how documents were kept in the usual course of business; by converting files to TIFF, defendant altered the documents and removed their metadata); *In re Priceline.com Inc. Sec. Litig.*, 233 F.R.D. 88, 91 (D. Conn. 2005) (ordering production in TIFF or PDF since those formats provided "the most secure format for the production of documents," but requiring that original data be maintained in native format for the duration of the litigation in case the requesting party sought its production so as to "comprehend the information in the file."); *In re Verisign, Inc. Sec. Litig.*, No. C 02-02270 JW, 2004 WL 2445243, at \*1 (N.D. Cal. Mar. 10, 2004) (ordering production of e-mail in its native ".pst" format, and not in TIFF format as had been requested by the producing party).

<sup>9</sup> See, e.g., *Rodriguez*, 2006 WL 903675, at \*3; *Hagenbuch*, 2006 WL 665005, at \*2-3; *In re Priceline.com*, 233 F.R.D. at 91; *In re Verisign*, 2004 WL 2445243, at \*1-2.

<sup>10</sup> 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.

<sup>11</sup> *The Sedona Conference Glossary: E-Discovery & Digital Information Management* 28 (The Sedona Conference Working Group Series, May 2005) ("Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden or embedded and unavailable to computer users who are not technically adept. Metadata is generally not reproduced in full form when a document is printed."); *The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production* 5 (The Sedona Conference Working Group Series, July 2005) [hereinafter *The Sedona Principles*] ("Much metadata is not normally accessible by the computer user.").

<sup>12</sup> *The Sedona Principles*, *supra* note 11, at 5.

what makes metadata so hazardous.<sup>13</sup> Indeed, Google,<sup>14</sup> Dell,<sup>15</sup> Merck,<sup>16</sup> the United Nations Secretary General,<sup>17</sup> the Democratic National Committee,<sup>18</sup> and others<sup>19</sup> have recently made embarrassing and sometimes damaging revelations through inadvertent disclosures of metadata.

The legal profession has also suffered its share of inadvertent metadata disclosures.<sup>20</sup> Just last summer, electronically redacted excerpts from a U.S. Justice Department brief became publicly viewable after they were copied and inserted into a Microsoft Word document.<sup>21</sup> Despite the fact that some

---

<sup>13</sup> See *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age* 82 (The Sedona Conference Working Group Series, Sept. 2005) [hereinafter *The Sedona Guidelines*] (“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.”); see also Ball, *supra* note 10, at 36 (characterizing metadata as “the electronic equivalent of DNA, ballistics and fingerprint evidence, with a comparable power to exonerate and incriminate. Metadata sheds light on the context, authenticity, reliability and dissemination of electronic evidence, as well as providing clues to human behavior.”).

<sup>14</sup> See Verne Kopytoff, *Google’s Gaffe Reveals Internal Secrets: Notes Inadvertently Offer a Look at Financial Plans, Future Product*, S.F. CHRON., Mar. 8, 2006, at C1, available at <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2006/03/08/GOOGLE.TMP>.

<sup>15</sup> See Tom Krazit, *Slip-up Spills Beans on Dell Notebooks*, CNET NEWS.COM, Feb. 1, 2006, [http://news.com.com/Slip-up+spills+beans+on+Dell+notebooks/2100-1044\\_3-6033903.html](http://news.com.com/Slip-up+spills+beans+on+Dell+notebooks/2100-1044_3-6033903.html).

<sup>16</sup> See David M. Ewalt, *When Words Come Back From The Dead*, FORBES.COM, Dec. 13, 2005, [http://www.forbes.com/2005/12/13/microsoft-word-merck\\_cx\\_de\\_1214\\_word.html](http://www.forbes.com/2005/12/13/microsoft-word-merck_cx_de_1214_word.html).

<sup>17</sup> See James Bone & Nicholas Blanford, *UN Office Doctored Report on Murder of Hariri*, TIMES (LONDON), Oct. 22, 2005, at 2, available at <http://www.timesonline.co.uk/article/0,251-1837848,00.html>.

<sup>18</sup> 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>.

<sup>19</sup> Up to date and historical information on metadata disclosures can be found at <http://www.metadatarisk.org> (follow “Content Security News” hyperlink) (last visited Feb. 5, 2007).

<sup>20</sup> In 2004, metadata from a draft letter apparently released by then California Attorney General Bill Lockyer’s office, which criticized the practices of peer-to-peer networking companies, showed that a prior draft was created by the Motion Picture Association of America. John Borland, *P2P Faces New Legal Scrutiny from States*, CNET NEWS.COM, Mar. 15, 2004, [http://news.com.com/P2P+faces+new+legal+scrutiny+from+states/2100-1038\\_3-5173262.html](http://news.com.com/P2P+faces+new+legal+scrutiny+from+states/2100-1038_3-5173262.html).

<sup>21</sup> 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>.

attorneys have known about the significance of metadata for years,<sup>22</sup> until recently there have been only a few court decisions discussing its import or requiring its disclosure.<sup>23</sup> That is no longer the case, however. During the past two years, courts around the nation have ordered production of metadata.<sup>24</sup> Such decisions recognize the value of metadata in establishing and ensuring document integrity and reliability.<sup>25</sup> This trend will likely continue under the 2006 amendments to the Federal Rules of Civil Procedure, which arguably impose a modest presumption in favor of preserving and producing relevant metadata.<sup>26</sup>

Given metadata's developing significance in the legal profession, and especially in litigation, there is a substantial need for attorneys to understand what metadata is, as well as its potential magnitude in a case.<sup>27</sup> Part Two of this Article will address these issues. In particular, I 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. Part Three of this Article will

---

<sup>22</sup> See *Armstrong v. Executive Office of the President*, 1 F.3d 1274, 1285 (D.C. Cir. 1993) (recognizing the basic characteristics of e-mail metadata).

<sup>23</sup> *Id.* at 1280, 1284-85; *Momah v. Albert Einstein Med. Ctr.*, 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).

<sup>24</sup> *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).

<sup>25</sup> *Rodriguez*, 2006 WL 903675, at \*3; *Hagenbuch*, 2006 WL 665005, at \*2; *Krumwiede v. Brighton Assoc.*, No. 05 C 3003, slip op. at 5-6, 10-11 (N.D. Ill. May 8, 2006), available at 2006 WL 1308629; *In re Telxon Corp. Sec. Litig.*, No. 5:98CV2876, 1:01CV1078, 2004 WL 3192729 (N.D. Ohio July 16, 2004), reported in LexisNexis as *Hayman v. Price Waterhouse Coopers, LLP*, 2004 U.S. LEXIS 27296; *CP Solutions PTE, Ltd. v. General Elec. Co.*, No. 3:04cv2150(JBA)(WIG), slip op. at 4 (D. Conn. 2006), available at 2006 WL 1272615.

<sup>26</sup> See *infra* Part IV.B.

<sup>27</sup> See, e.g., *Zubulake v. UBS Warburg LLC (Zubulake V)*, 229 F.R.D. 422, 440 (S.D.N.Y. 2004) ("Now that the key issues have been addressed and national standards are developing, parties and their counsel are fully on notice of their responsibility to preserve and produce electronically stored information.").

2007]                      *PRESERVING AND OBTAINING METADATA*

review the case law addressing the preservation and production of metadata and discuss the predominant theme—document integrity—that courts have trumpeted in ordering that metadata be produced. Part Four will discuss whether the current trend favoring production of metadata will continue now that the amendments to the Federal Rules of Civil Procedure have been implemented. Lastly, Part Five will propose some useful practice tips relating to preserving and obtaining metadata.

II. THE NATURE AND SIGNIFICANCE OF METADATA

As mentioned in Part One, metadata is digitally stored information about a document’s characteristics, including its origin and usage.<sup>28</sup> 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 counsel and clients typically include Microsoft Word, Adobe Portable Document Format (“PDF”), e-mail, Microsoft Excel and Corel Word Perfect.

A. *Electronic Documents Containing Metadata*

1. Metadata in Microsoft Word

Microsoft Word documents contain metadata that can be both helpful and harmful to a user.<sup>29</sup> 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.<sup>30</sup> Of these features, the

---

<sup>28</sup> Ball, *supra* note 10, at 36.

<sup>29</sup> See Payne, *Metadata – Are you Protected?*, *supra* note 2, at 1; 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*].

<sup>30</sup> *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 29, at 80.

“track changes” function is perhaps the most significant.<sup>31</sup>

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.<sup>32</sup> However, such transparency is precisely what makes the track changes feature so problematic.<sup>33</sup> 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.<sup>34</sup> 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.<sup>35</sup>

---

<sup>31</sup> See Zeller, *supra* note 18, at C5; 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](http://news.com.com/Hidden+text+shows+SCO+prepped+lawsuit+against+BofA/2100-7344_3-5170073.html).

<sup>32</sup> 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.”).

<sup>33</sup> See Shankland, *supra* note 31.

<sup>34</sup> *Id.*

<sup>35</sup> See, e.g., Payne, *Metadata – Are you Protected?*, *supra* note 2, at 3; Payne, *Metadata: The Good, the Bad, and the Ugly*, *supra* note 29, at 80, 82; Beckham, *supra* note 30, 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. The Florida Bar is considering issuing a similar opinion. 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 those jurisdictions, 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*

2007] PRESERVING AND OBTAINING METADATA

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.<sup>36</sup> 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.<sup>37</sup>

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.<sup>38</sup> 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, which contains no metadata.<sup>39</sup> While its contents may or may not be altered, a PDF can still contain metadata.<sup>40</sup> For example, unless appropriate precautions are taken, PDF metadata may include data imported from the original Word document.<sup>41</sup> This could include *all* of the "comments and tracked changes if they are contained in the original document."<sup>42</sup> PDF files also contain information about the file author, the date the file was created and modified, and a summary of the document.<sup>43</sup>

---

*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](http://www.abanet.org/abanet/media/release/news_release.cfm?releaseid=48).

<sup>36</sup> Payne, *Metadata: The Good, the Bad, and the Ugly*, *supra* note 29, at 80.

<sup>37</sup> See Walker, *supra* note 35. Irrespective of the ethical implications, counsel should take measures 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 & 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").

<sup>38</sup> Payne, *Metadata – Are you Protected?*, *supra* note 2, at 2; Payne, *Metadata: The Good, the Bad, and the Ugly*, *supra* note 29, at 83.

<sup>39</sup> Payne, *Metadata – Are you Protected?*, *supra* note 2, at 2; Payne, *Metadata: The Good, the Bad, and the Ugly*, *supra* note 29, at 83.

<sup>40</sup> Payne, *Metadata – Are you Protected?*, *supra* note 2, at 2; Payne, *Metadata: The Good, the Bad, and the Ugly*, *supra* note 29, 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](http://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_PDF_TrumpsTIFF.pdf) (last visited Aug. 28, 2006).

<sup>41</sup> Applied Discovery, *supra* note 40, at 3.

<sup>42</sup> See Payne, *Metadata: The Good, the Bad, and the Ugly*, *supra* note 29, at 83.

<sup>43</sup> *Id.*

### 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.”<sup>44</sup> This 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.<sup>45</sup>

As a Microsoft application, Excel contains much of the same metadata found in Word, including author and revision history information.<sup>46</sup> 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.”<sup>47</sup>

Word Perfect contains some of the same strains of metadata found in Word.<sup>48</sup> 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.<sup>49</sup> 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.<sup>50</sup>

#### B. Dealing with the Hazards of Metadata

As many attorneys and their clients know, the danger of disclosing metadata in interrogatory responses is not merely hypothetical.<sup>51</sup> For instance, when the

---

<sup>44</sup> Beckham, *supra* note 30, at 4.

<sup>45</sup> Armstrong v. Executive Office of the President, 1 F.3d 1274, 1280, 1284 (D.C. Cir. 1993); Sharon Nelson and John Simek, *Metadata: What You Can’t See Can Hurt You*, 32 No. 2 LAW PRAC. 28, 29 (Mar 2006); *The Sedona Principles*, *supra* note 11, at 5.

<sup>46</sup> Microsoft, *How to Minimize Metadata in Microsoft Excel Workbooks*, <http://support.microsoft.com/kb/223789/en-us> (last visited Aug. 28, 2006).

<sup>47</sup> *The Sedona Principles*, *supra* note 11, at 5; *see also* Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 647 (D. Kan. 2005).

<sup>48</sup> Payne, *Metadata – Are you Protected?*, *supra* note 2, at 2; Payne, *Metadata: The Good, the Bad, and the Ugly*, *supra* note 29, at 79-80.

<sup>49</sup> Payne, *Metadata: The Good, the Bad, and the Ugly*, *supra* note 29, 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>.

<sup>50</sup> *See* Pinnington, *supra* note 49, at 36-37.

<sup>51</sup> *See* Shankland, *supra* note 31.

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.<sup>52</sup> 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.<sup>53</sup> That sophisticated technology companies such as SCO have inadvertently disclosed attorney work product further underscores the importance of understanding and addressing the dangers of metadata.<sup>54</sup>

Despite its troublesome nature, metadata can often be managed with appropriate precautions.<sup>55</sup> 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 floppy disks, flash drives, CD-ROMs or DVD-ROMs.<sup>56</sup> Accordingly, counsel may control the flow of metadata by monitoring and controlling the materials that leave the office.<sup>57</sup> 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.<sup>58</sup> 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.<sup>59</sup> Electronic discovery consultants may also be retained to advise how to recognize problematic metadata and to assist in removing it from electronic documents. Like most difficulties in the practice of law, the problem of metadata is not intractable and can be managed with appropriate care.<sup>60</sup>

### C. *The Value of Metadata*

Once appropriate steps are taken to control the hazards of metadata, its value

---

<sup>52</sup> *Id.*

<sup>53</sup> *Id.*

<sup>54</sup> 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 30, at 3.

<sup>55</sup> Pinnington, *supra* note 49, at 37; Payne, *Metadata – Are you Protected?*, *supra* note 2, at 3-4.

<sup>56</sup> *See* Pinnington, *supra* note 49, at 37.

<sup>57</sup> *See id.*

<sup>58</sup> Various vendors, including the Payne Consulting Group, offer a number of these products for sale. *See id.*

<sup>59</sup> *See* Applied Discovery, *supra* note 40.

<sup>60</sup> Pinnington, *supra* note 49, at 37; Payne, *Metadata – Are you Protected?*, *supra* note 2, at 3-4.

may be realized.<sup>61</sup> One of the significant benefits of metadata is its usefulness in authenticating documents.<sup>62</sup> 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.<sup>63</sup> 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.<sup>64</sup>

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.<sup>65</sup> Indeed, most court decisions addressing the significance of metadata have recognized its value in demonstrating document integrity.<sup>66</sup> The inherent traits

---

<sup>61</sup> See Ball, *supra* note 10, at 36.

<sup>62</sup> *Id.*; see also *The Sedona Principles*, *supra* note 11, at 5.

<sup>63</sup> Ball, *supra* note 10, at 36; *The Sedona Principles*, *supra* note 11, at 5; see also, e.g., FED. R. EVID. 901; CAL. EVID. CODE §§ 1400-1402 (West 2006).

<sup>64</sup> See *The Sedona Principles*, *supra* note 11, at 5.

<sup>65</sup> *Id.* at 46; *Plasse v. Tyco Elecs. 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 Am., 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).

<sup>66</sup> See *Armstrong v. Executive Office of the President*, 1 F.3d 1274, 1280, 1284-85 (D.C. Cir. 1993); *Momah v. Albert Einstein Med. Center*, 164 F.R.D. 412, 418 (E.D. Pa. 1996); *In re* 3817 W. West End, First Floor Chicago, Ill. 60621, 321 F. Supp. 2d 953, 956 n.1 (N.D. Ill. 2004); *CP Solutions PTE, Ltd. v. General Elec. Co.*, No. 3:04cv2150 (JBA)(WIG), 2006 WL 1272615, at \*10-11 (D. Conn. Feb. 2, 2006); *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); *Krumwiede v. Brighton Assoc.*, No. 05 C 3003, slip op. at 20-21 (N.D. Ill. May 8, 2006), *available at* 2006 WL 1308629; *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); *In re* Telxon Corp. Sec. Litig., No. 5:98CV2876, 1:01CV1078, 2004 WL 3192729, at \*22, \*34 (N.D. Ohio July 16, 2004); *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640, 647 (D. Kan. 2005).

2007]                    *PRESERVING AND OBTAINING METADATA*

of metadata also make it an effective document management device<sup>67</sup> and “useful for system administration as it reflects data regarding the generation, handling, transfer, and storage of the data within the computer system.”<sup>68</sup>

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.<sup>69</sup> 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.<sup>70</sup> This technique allowed the company to manage the flow of privileged information and ascertain the loyalty of its employees.<sup>71</sup>

*D. Understanding Metadata Enhances Effective Client Representation*

In summary, 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 properly understood and utilized, metadata can provide tremendous value for companies in their respective fields and an enormous advantage for attorneys in litigation. However, when metadata is unknown, ignored or not properly controlled, counsel and client may encounter problems they could have otherwise avoided.

III. RECENT CASE LAW DEVELOPMENTS ON PRODUCTION OF METADATA

The decisions issued in 2006 requiring production of metadata have been as significant in their numbers as they have been in their content. Prior to 2006, there were very few decisions even discussing metadata, let alone requiring its preservation or production. While few in number, those pre-2006 decisions were nonetheless significant because they established the predominant theme associated with metadata preservation and production: document integrity. This Part will explore the development of this theme in pre-2006 case law and then discuss its role in metadata decisions from 2006. This Part will also touch on cases in which courts have ordered production of metadata based on the “production in the usual course” requirement of Federal Rule of Civil

---

<sup>67</sup> Pinnington, *supra* note 49, at 36.

<sup>68</sup> *The Sedona Principles*, *supra* note 11, at 5.

<sup>69</sup> *The Sedona Guidelines*, *supra* note 14, at 80.

<sup>70</sup> *Toftely v. Qwest Commc's 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).

<sup>71</sup> *Id.*

Procedure 34(b)(i)<sup>72</sup>.

A. *Notable Pre-2006 Case Law – Armstrong, Telxon and Williams*

One of the earliest cases to recognize the significance of metadata in terms of document integrity is *Armstrong v. Executive Office of the President*.<sup>73</sup> In that 1993 decision, the court held that the Federal Records Act requires certain executive branch agencies to archive the electronic version of its e-mail.<sup>74</sup> The defendants unsuccessfully argued that e-mail print-outs were the logical equivalent of electronic material, and consequently there should be no obligation to archive superfluous electronic “copies.”<sup>75</sup> In rejecting that argument, the court found printed computer records, particularly printed e-mail, do not display all of the information contained in electronic documents.<sup>76</sup> Without specifically mentioning the term “metadata,” the court detailed some of the embedded information found in e-mail that often cannot be viewed in hard copy: “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.”<sup>77</sup> By failing to include electronic materials in its archived records, the defendants’ files comprised an incomplete record, replete with what the court characterized as “dismembered documents” and “amputated paper print-outs.”<sup>78</sup>

The *Armstrong* decision is noteworthy for several reasons. While there were other decisions that previously acknowledged the primacy of digital material over hard copies,<sup>79</sup> the *Armstrong* court was perhaps the first to recognize the role of metadata in establishing that pecking order. It is noteworthy that the court did so in the context of e-mail, since e-mail was not a widespread form of communication at that time. More significantly, *Armstrong*’s justification for preserving electronic data was prescient. Its

---

<sup>72</sup> FED. R. CIV. P. 34(b)(i) (“a party who produces documents for inspection shall produce them as they are kept in the usual course of business or shall organize and label them to correspond with the categories in the request”).

<sup>73</sup> *Armstrong v. Executive Office of the President*, 1 F.3d 1270 (D.C. Cir. 1993).

<sup>74</sup> *Id.* at 1283.

<sup>75</sup> *Id.* at 1284-85.

<sup>76</sup> *Id.* at 1277, 1280, 1284-85.

<sup>77</sup> *Id.* at 1284 (emphasis added).

<sup>78</sup> *Id.* at 1285.

<sup>79</sup> *See, e.g., In re Air Crash Disaster at Detroit Metro. Airport on Aug. 16, 1987*, 130 F.R.D. 634, 636 (E.D. Mich. 1989); *Daewoo Elec. Co. v. United States*, 10 Ct. Int’l Trade 754, 757 (1986); *Nat’l Union Elec. Corp. v. Matsushita Elec. Indus. Co.*, 494 F. Supp. 1257, 1262 (E.D. Pa. 1980).

2007] PRESERVING AND OBTAINING METADATA

rationale serves as a foundation for modern views on the preservation and production of metadata, particularly in the context of e-mail.<sup>80</sup>

In sharp contrast to the advisory nature of *Armstrong* stands the cautionary holding regarding metadata preservation in *In re Telxon Corp. Securities Litigation*.<sup>81</sup> In *Telxon*, a magistrate recommended default judgment be entered against the defendant for various irregularities relating to its preservation and production of documents.<sup>82</sup> In particular, the court spotlighted the defendant's failure to preserve metadata as a basis for its decision.<sup>83</sup> This holding teaches that parties arguably have an obligation to preserve and conceivably produce documents' metadata.

Just as important in *Telxon*, however, was the role metadata played in exposing concealed modifications to the defendant's records.<sup>84</sup> The records' file histories showed the defendant had altered certain documents after being advised not to do so.<sup>85</sup> This misconduct factored into the *Telxon* court's recommended sanctions, and demonstrates the role metadata can play in establishing a document's authenticity.<sup>86</sup>

The significance of *Telxon* cannot be understated, particularly since it was cited as precedent in the 2005 case of *Williams v. Sprint/United Management Co.*, one of the few reported decisions to order production of metadata.<sup>87</sup> In *Williams*, the court ordered the defendant to produce metadata embedded in Excel spreadsheets that had been removed prior to the spreadsheets' initial production.<sup>88</sup> Not only was the metadata discoverable because it was relevant to the plaintiffs' claims; its removal impugned the integrity of the document: "*a spreadsheet's metadata may be necessary to understand the spreadsheet because the cells containing formulas, which arguably are metadata themselves, often display a value rather than the formula itself. To understand the spreadsheet, the user must be able to ascertain the formula within the*

---

<sup>80</sup> See Applied Discovery, *Embedded Information in Electronic Documents: Why Meta Data Matters*, at 1-2, [http://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI\\_MetaData.pdf](http://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_MetaData.pdf) (last visited Aug. 28, 2006).

<sup>81</sup> *In re Telxon Corp. Sec. Litig.*, No. 5:98CV2876, 1:01CV1078, 2004 WL 3192729, at \*34-35 (N.D. Ohio July 16, 2004).

<sup>82</sup> *Id.* at \*35-36.

<sup>83</sup> *Id.* at \*34 ("missing metadata . . . suggest that PwC may be withholding or has improperly destroyed discoverable information.").

<sup>84</sup> *Id.*

<sup>85</sup> *Id.* at \*22, \*34.

<sup>86</sup> *Id.* at \*34-36.

<sup>87</sup> *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640, 650 (D. Kan. 2005).

<sup>88</sup> *Id.* at 653, 657.

cell.”<sup>89</sup>

*Williams* is a watershed decision because it represents the first instance in a published case where a party was specifically compelled to produce metadata. *Williams* was not an isolated event; a few months later, in another published decision, a party was ordered to produce “searchable metadata databases.”<sup>90</sup> Since 2004, other courts have likewise acknowledged the importance of metadata.<sup>91</sup> Some courts have ordered documents produced in “native format” so as to capture their metadata.<sup>92</sup> Still others have recognized the discoverability of metadata<sup>93</sup> and issued protective orders to preserve it.<sup>94</sup>

*B. Significant 2006 Case Law: Hagenbuch and Krumwiede*

The principal case from 2006 addressing metadata production is undoubtedly *Hagenbuch v. 3B6 Sistemi Elettronici Industriali S.R.L.*<sup>95</sup> In *Hagenbuch* (a patent infringement case), the court held that parties have an obligation under Rule 34 of the Federal Rules of Civil Procedure to produce digital materials in their native format in order to ensure production of relevant metadata.<sup>96</sup> The issue arose after the defendants converted electronic media they had agreed to produce into TIFF documents.<sup>97</sup> The court found the TIFF production was insufficient under Rule 34’s production in the “ordinary

---

<sup>89</sup> *Id.* at 647 (emphasis added).

<sup>90</sup> *In re Priceline.com, Inc. Sec. Litig.*, 233 F.R.D. 88, 91 (D. Conn. 2005).

<sup>91</sup> *See, e.g., In re 3817 W. West End, First Floor Chicago, Ill.* 60621, 321 F. Supp 2d 953, 956 n.1 (N.D. Ill. 2004); *Wild v. Alster*, 377 F. Supp. 2d 186, 194-95 (D.D.C. 2005); *Quinby v. WestLB AG, No. 04Civ.7406 (WHP)(HBP)*, 2005 WL 3453908, at \*6 (S.D.N.Y. Dec. 15, 2005) (recognizing the need to retain an expert in order to conduct a complete search of a database and its metadata).

<sup>92</sup> *See In re Pemstar, Inc. Sec. Litig.*, Civil No. 02-1821 (DWF/SRN), \*2-6 (D. Minn. 2004) (ordering production in native format since it would efficiently use metadata to facilitate searches of defendants’ e-mails and corresponding attachments); *In re Verisign, Inc. Sec. Litig.*, No. C 02-02270 JW, 2004 WL 2445243, at \*1-2 (implying that Rule 34’s “ordinary course” requirement called for production of metadata).

<sup>93</sup> *See Hopson v. Mayor & City Council of Baltimore*, 232 F.R.D. 228, 245 (D. Md. 2005) (suggesting that parties should discuss production of metadata in their discovery conference); *In re Vioxx Prod. Liab. Litig.*, No. MDL 1657, 2005 WL 756742, at \*3 (E.D. La. 2005) (directing in its pretrial order that the parties preserve all relevant evidence, including metadata).

<sup>94</sup> *Pueblo of Laguna v. United States.*, 60 Fed. Cl. 133, 141 (2004); *Jicarilla Apache Nation v. United States*, 60 Fed. Cl. 413, 414 (2004).

<sup>95</sup> *Hagenbuch v. 3B6 Sistemi Elettronici Industriali S.R.L.*, No. 04 C 3109, 2006 WL 665005 (N.D. Ill. Mar. 8, 2006).

<sup>96</sup> *Id.* at \*2.

<sup>97</sup> *Id.* at \*1.

2007] PRESERVING AND OBTAINING METADATA

course” requirement, since TIFF documents do not contain metadata:

[I]t is clear that the TIFF documents do not contain all of the relevant, nonprivileged information contained in the designated electronic media. The parties agree that, unlike the original electronic media . . . the TIFF documents do not contain information such as the creation and modification dates of a document, e-mail attachments and recipients, and metadata.<sup>98</sup>

Moreover, by converting the media to TIFF documents and removing the metadata, the defendant altered the records and “essentially created new documents” for production.<sup>99</sup> Such a production, which removed information relevant to the plaintiff’s claims, did not comply with Rule 34.<sup>100</sup> Only by making the documents available in the same format in which they were kept could the defendant meet its Rule 34 production obligations.<sup>101</sup> The *Hagenbuch* holding expresses what earlier cases merely implied: Rule 34 requires production of relevant metadata.<sup>102</sup> *Hagenbuch* also reinforced the holdings from *Armstrong* and *Williams* that metadata is an integral part of a document and its removal impugns a document’s genuineness.<sup>103</sup>

*Hagenbuch* examined the issue of metadata and document integrity in connection with a motion to compel.<sup>104</sup> Another 2006 case, *Krumwiede v. Brighton Associates*, analyzed the same concept in the context of a motion for sanctions.<sup>105</sup> In *Krumwiede*, a wrongful termination and trade secret misappropriation case, the plaintiff systematically altered and purged metadata from his computer in order to conceal his removal of proprietary electronic files from his former employer.<sup>106</sup> By modifying and destroying the metadata, the plaintiff permanently changed the character of certain key documents and made it impossible for the defendant to establish their authenticity.<sup>107</sup> Because

---

<sup>98</sup> *Id.* at \*2, \*3.

<sup>99</sup> *Id.* at \*2.

<sup>100</sup> *Id.*

<sup>101</sup> *Id.*

<sup>102</sup> See *In re Verisign, Inc. Sec. Litig.*, No. C 02-02270 JW, 2004 WL 2445243, at \*2 (N.D. Cal. Mar. 10, 2004).

<sup>103</sup> See *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640, 647 (D. Kan. 2005); *Armstrong v. Executive Office of the President*, 1 F.3d 1274, 1280, 1284-85 (D.C. Cir. 1993).

<sup>104</sup> See *Hagenbuch v. 3B6 Sistemi Elettronici Industriali S.R.L.*, No. 04 C 3109, 2006 WL 665005 \*1 (N.D. Ill. Mar. 8, 2006)

<sup>105</sup> *Krumwiede v. Brighton Assoc., L.L.C.*, No. 05 C 3003, slip op. at 21-22 (N.D. Ill. May.8, 2006).

<sup>106</sup> *Id.* at 7-14.

<sup>107</sup> *Id.* at 20-21.

removal of the metadata compromised the genuineness of the documents and foreclosed the defendant from proving its counterclaims, a sanction of default judgment against the plaintiff was appropriate.<sup>108</sup> Just like the result in *Telxon, Krumwiede* teaches that harsh sanctions are justified for the spoliation of metadata.<sup>109</sup> These cases suggest that parties have an obligation to preserve relevant metadata once litigation is reasonably foreseeable.<sup>110</sup>

In addition to *Hagenbuch* and *Krumwiede*, several other 2006 decisions have focused on the production of metadata. For example, in *Nova Measuring Instruments Ltd. v. Nanometrics* and *In re NYSE Specialists Securities Litigation*, both courts ordered production of electronic records in native format, including the metadata corresponding to the records.<sup>111</sup> In *Rodriguez v. City of Fresno*, the defendants were ordered to produce metadata corresponding to certain police reports so that the plaintiffs could determine the nature of any changes made to those documents.<sup>112</sup> Finally, in *CP Solutions PTE, Ltd. v. General Electric Co.*, the defendant was ordered to produce metadata that would allow the plaintiff to link up e-mails produced by the defendant with their respective attachments.<sup>113</sup>

C. *The Continued Viability of Metadata Case Law is Largely Dependant on the Newly Amended Federal Rules of Civil Procedure*

With the number and nature of metadata-related decisions issued over the past two years, a judicial trend appears to be developing in favor of imposing a duty on parties to preserve and produce relevant metadata once litigation is reasonably foreseeable. The continuation of this trend, however, largely depends on judicial interpretation of the newly amended Federal Rules of Civil Procedure, which deal with electronic discovery issues. Those amendments, particularly the amendments to Rule 34, impose new ground rules that will likely affect the preservation and production of metadata. These issues will be

---

<sup>108</sup> *Id.*

<sup>109</sup> *Id.* at 21.

<sup>110</sup> *Id.* at 15-16.

<sup>111</sup> *Nova Measuring Instruments Ltd. v. Nanometrics, Inc.*, 417 F. Supp. 2d 1121, 1122 (N.D. Cal. 2006); *In re NYSE Specialists Sec. Litig.*, No. 03 Civ. 8264(RWS), 2006 WL 1704447, at \*1 (S.D.N.Y. June 14, 2006).

<sup>112</sup> *Rodriguez v. City of Fresno*, No. 1:05cv1017 OWW DLB, 2006 WL 903675, at \*3 (E.D. Cal. Apr. 7, 2006).

<sup>113</sup> *CP Solutions PTE, Ltd. v. General Elec. Co.*, No. 3:04cv2150 (JBA)(WIG), slip op. at 11 (D. Conn. Feb. 6, 2006), available at 2006 WL 1272615. In another 2006 decision, a federal district court found evidence of copyright infringement based on certain metadata, which showed the defendant illegally distributed the plaintiff's motion picture. *Paramount Pictures Corp. v. Davis*, Civil Action No. 05-0316, 2006 WL 2092581, at \*4 (E.D. Pa. July 26, 2006).

explored in the following Part.

#### IV. AMENDMENTS TO THE FEDERAL RULES OF CIVIL PROCEDURE AND THEIR IMPACT ON METADATA PRESERVATION AND PRODUCTION

The amended Federal Rules of Civil Procedure, which include changes to Rules 16, 26, 33, 34, 37, 45 and Form 35, are designed to alleviate certain challenges posed by electronically stored information that the rules did not previously address.<sup>114</sup> While the amendments do not expressly discuss metadata production and preservation, they have been drafted to provide general guidance to litigants on such issues.<sup>115</sup>

##### A. *Amendments to Rules 16, 26(a) and 26(f) — Addressing Metadata Issues Early in the Litigation*

Amended Rule 26(a)'s requirement that parties produce "electronically stored information" in connection with their initial disclosures suggests that metadata corresponding to those electronic files should also be produced if known to be relevant to the claims at issue.<sup>116</sup> The amendment to Rule 26(f) directs litigants to confer on issues relating to discovery of digital material, including preservation of electronic evidence and designation of document production formats.<sup>117</sup> As the Advisory Committee notes, this provides the parties with an avenue to raise and address issues relating to metadata preservation and production.<sup>118</sup> Furthermore, under amended Rule 16, courts

---

<sup>114</sup> See JUDICIAL CONFERENCE OF THE UNITED STATES, REPORT OF THE JUDICIAL CONFERENCE COMMITTEE ON RULES OF PRACTICE AND PROCEDURE 23-24 (Sept. 2005), available at <http://www.uscourts.gov/rules/Reports/ST09-2005.pdf> [hereinafter REPORT]. The amendments became effective on December 1, 2006. See Leigh Jones, *E-Discovery Zero Hour Approaching*, NAT'L L. J., Aug. 18, 2006, <http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1155892468834>.

<sup>115</sup> For example, the Advisory Committee note to the 2006 Amendments to Rule 34(a) indicate that the changes were "intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments." REPORT, *supra* note 114, at app. C-74.

<sup>116</sup> *Id.* at 26; *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640, 654 (D. Kan. 2005) ("Of course, if the producing party knows or should reasonably know that particular metadata is relevant to the dispute, it should be produced."), quoting *The Sedona Principles*, *supra* note 11, at 46.

<sup>117</sup> REPORT, *supra* note 114, at 26-27.

<sup>118</sup> *Id.* at app. C-35-36 ("For example, production may be sought of information automatically included in electronic files but not apparent to the creator or to readers. Computer programs may retain draft language, editorial comments, and other deleted matter (sometimes referred to as "embedded data" or "embedded edits") in an electronic file but not make them apparent to the reader. Information describing history, tracking, or

can set ground rules in a scheduling order regarding the preservation and disclosure of electronically stored information, including metadata.<sup>119</sup>

*B. Amendments to Rule 34 — Implied Right to Obtain Relevant Metadata*

Assuming, however, that neither the parties nor the court avail themselves of these new discovery devices, the amendments to Rule 34 may have a significant effect on metadata production. Like the other amended discovery rules, amended Rule 34 was expressly drafted to recognize that electronic data is subject to discovery and should be treated differently from paper documents.<sup>120</sup> Electronic materials are now distinctly characterized as “electronically stored information” instead of being classified as a mere subset of “documents.”<sup>121</sup> This distinction creates a set of discovery rights and obligations for electronic data different than those for paper documents.<sup>122</sup>

For instance, amended Rule 34(b) allows the requesting party to specify a particular form for production of electronic documents.<sup>123</sup> Such a right may enable a party to obtain metadata either by requesting that productions be made in native format or in TIFF with corresponding databases containing extracted metadata.<sup>124</sup> And while the responding party may object to the form of production and elect not to produce the metadata, nothing in the amendments forecloses the requesting party from seeking its production through a motion to compel.<sup>125</sup>

If, on the other hand, the requesting party does not specify a form for production, the responding party may not produce electronic materials in a form that makes the documents more difficult to review.<sup>126</sup> As the Advisory Committee makes clear:

*Producing electronically stored information with the ability to search by electronic means removed or degraded is the electronic discovery version of the “document dump,” the production of large amounts of paper with no organization or order . . . [i]f the responding party ordinarily maintains*

---

management of an electronic file (sometimes called “metadata”) is usually not apparent to the reader viewing a hard copy or a screen image. Whether this information should be produced may be among the topics discussed in the Rule 26(f) conference.”)

<sup>119</sup> *Id.* at 26.

<sup>120</sup> *Id.*

<sup>121</sup> *Id.* at app. C-65.

<sup>122</sup> *Id.*

<sup>123</sup> *Id.* at app. C-76.

<sup>124</sup> *See, e.g.,* 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).

<sup>125</sup> REPORT, *supra* note 114, at app. C-77.

<sup>126</sup> *Id.* at app. C-67, C-77.

2007] PRESERVING AND OBTAINING METADATA

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.<sup>127</sup>

Given the vital role that metadata plays in document management, this provision suggests that removal of metadata prior to production may be prohibited, and creates a presumption that relevant metadata must be produced in discovery.<sup>128</sup> Such an amendment would seem to increase a party's chance to obtain metadata, even if the party neglected to specifically request it.<sup>129</sup>

C. *New Rule 37(f) — Safe Harbor against Sanctions for Metadata Spoliation*

New Rule 37(f) creates a safe harbor which shields litigants from sanctions for evidence spoliation where electronic data (including metadata) has been recycled in good faith pursuant to the “routine operation of an electronic information system.”<sup>130</sup> This provision is intended to protect parties from the incidental alteration or deletion of electronically stored information that frequently results from the “distinctive” nature of computer operations:

Many steps essential to computer operation may alter or destroy information, for reasons that have nothing to do with how that information might relate to litigation. As a result, the ordinary operation of computer systems creates a risk that a party may lose potentially discoverable information without culpable conduct on its part . . . . *The “routine operation” of computer systems includes the alteration and overwriting of information, often without the operator’s specific direction or awareness, a feature with no direct counterpart in hard-copy documents.*<sup>131</sup>

Accordingly, even relevant electronic records and metadata can be recycled

---

<sup>127</sup> *Id.* at app. C-67 (emphasis added).

<sup>128</sup> Not surprisingly, courts will likely decline to order production of metadata if a party fails to show that metadata is within the permissible scope of discovery. *See Kentucky Speedway, LLC v. Nat’l Assoc. of Stock Car Auto Racing, Inc.*, No. 2:05-CV-00138-WOB, slip op. at 12 (E.D. Ky. Dec. 18, 2006) (declining to order production of metadata since the requesting party failed to make “any showing of a particularized need for metadata”); *Wyeth v. Impax Laboratories, Inc.*, No. Civ.A. 06-222-JJF, slip op. at 1-2 (D. Del. October 26, 2006), *available at* 2006 WL 3091331 (denying defendant’s request for production of documents in “native format, complete with metadata” since no “particularized need” was established for that information).

<sup>129</sup> This would seem to violate one of the law’s sacred maxims: “The law helps those that help themselves, generally aids the vigilant, but rarely the sleeping, and never the acquiescent.” *Hannan v. Dusch*, 153 S.E. 824, 831 (Va. 1931).

<sup>130</sup> FED. R. CIV. P. 37(f).

<sup>131</sup> REPORT, *supra* note 114, at app. C-86-87 (emphasis added).

and purged without sanctions, so long as it is done in good faith.<sup>132</sup> However, the safe harbor provision may not apply in “exceptional circumstances,” *e.g.*, where there is a common law or statutory duty to preserve evidence or a court-imposed preservation order exists, or where a party negligently (or intentionally) allows the routine operation of its computer information system to purge relevant electronic materials.<sup>133</sup>

D. *The Amended Rules Appear Consistent with Case Law Addressing Metadata Production and Preservation*

The changes effected by the new amendments do not appear to dramatically alter the landscape of metadata preservation and production. To the contrary, the amended rules seem in accord with various aspects of the *Hagenbuch*, *Krumwiede*, and *Telxon* decisions. Amended Rule 34(b), which allows a party to specify a form of production, is consistent with *Hagenbuch* since that court permitted the requesting party to specify the form of production—native format—that would contain metadata relevant to his infringement claims.<sup>134</sup> *Hagenbuch* also accords with amended Rule 34(b)’s stricture against certain types of data conversion, as the court recognized that the defendant’s conversion of native format documents to TIFF made the documents more difficult to search and review.<sup>135</sup>

Rule 37(f) also appears consonant with the holdings in *Krumwiede* and *Telxon*. In both of those decisions, the courts leveled doomsday sanctions against defendants who had intentionally modified and purged metadata despite having an obligation to preserve such information.<sup>136</sup> There should be little if any doubt that the parties’ gross misconduct in *Krumwiede* and *Telxon* would likely satisfy the “exceptional circumstances” sanctions requirement under Rule 37(f).<sup>137</sup> Given the arguable uniformity between existing metadata case law and the Federal Rules amendments, *Hagenbuch*, *Krumwiede* and *Telxon* continue to be instructive, and provide direction on metadata preservation and production under the amended rules.

---

<sup>132</sup> *Id.* (“Rule 37(f) applies to information lost due to the routine operation of an information system only if the operation was in good faith.”).

<sup>133</sup> *Id.*

<sup>134</sup> *See Hagenbuch v. 3B6 Sistemi Elettronici Industriali S.R.L.*, No. 04 C 3109, 2006 WL 665005, at \*3 (N.D. Ill. Mar. 8, 2006).

<sup>135</sup> *See id.* at \*2.

<sup>136</sup> *Krumwiede v. Brighton Assoc., L.L.C.*, No. 05 C 3003, slip op. at 21 (N.D. Ill. May 8, 2006); *In re Telxon Corp. Sec. Litig.*, No. 5:98CV2876, 1:01CV1078, 2004 WL 3192729, at \*34-36 (N.D. Ohio July 16, 2004).

<sup>137</sup> REPORT, *supra* note 114, at app. C-86-87.

2007]                    *PRESERVING AND OBTAINING METADATA*

V.    SUGGESTED PRACTICES FOR METADATA PRESERVATION AND PRODUCTION

In light of the developing body of case law and the amended Federal Rules of Civil Procedure, lawyers and litigants should adopt practices to ensure that relevant metadata is preserved and to obtain metadata information in discovery. This Part contains suggested practices that may be helpful in doing so.

A.    *Implement a Timely Litigation Hold*

Once litigation is reasonably foreseeable, counsel and client should take reasonable steps to implement a litigation hold and to determine what materials may be relevant or reasonably calculated to lead to admissible evidence.<sup>138</sup> In connection with this process, the client's computer information system and document retention policies should be examined to understand whether any relevant electronic records, including metadata, will be recycled and purged in the normal operation of that system.<sup>139</sup> This step is particularly important so as to determine whether any aspect of the information system and/or retention policies should be suspended to ensure that potentially relevant materials are retained.<sup>140</sup>

B.    *Check the Local Rules*

Before engaging in any type of discovery, litigants should determine whether there are local rules governing discovery of electronically stored information. In the absence of direction from the Federal Rules, many federal district courts proposed or adopted local rules to grapple with cumbersome electronic discovery issues.<sup>141</sup> Whether proposed or adopted, such rules may contain specific requirements or otherwise provide direction on preserving and obtaining electronically stored information (including metadata) in their

---

<sup>138</sup> *Zubulake v. UBS Warburg LLC (Zubulake V)*, 229 F.R.D. 422, 431-32 (S.D.N.Y. 2004); *see also* *Zubulake v. UBS Warburg LLC (Zubulake IV)*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003) (discussing the scope of a party's duty to preserve evidence once litigation is reasonably foreseeable); *Krumwiede*, slip op. at 17-18; *Telxon*, 2004 WL 3192729, at \*34.

<sup>139</sup> *See* *Zubulake V*, 229 F.R.D. at 432; *Zubulake IV*, 220 F.R.D. at 218; REPORT, *supra* note 114, at app. C-87.

<sup>140</sup> *See* *Zubulake V*, 229 F.R.D. at 432; *Zubulake IV*, 220 F.R.D. at 218; REPORT, *supra* note 114, at app. C-87.

<sup>141</sup> *See* Applied Discovery, Court Rules, <http://www.lexisnexis.com/applieddiscovery/lawLibrary/courtRules.asp> (last visited August 28, 2006) (discussing various local rules from Federal district courts as well as state court rules).

respective jurisdictions.<sup>142</sup>

*C. Determine and Specify the Form of Production*

Before propounding discovery or conducting the Rule 26(f) discovery conference, counsel should attempt to determine the most suitable form of production for the case. If, for instance, metadata is determined to be a vital source of information in the case, counsel should prepare discovery that expressly requests its production and should specify an electronic form (*e.g.*, native format or TIFF with metadata databases) that will most likely include the metadata. If counsel fails to expressly request the metadata or, even worse, does not specify a form of production, the client could lose the right to obtain such information.<sup>143</sup>

*D. Specifically Request “Electronically Stored Information”*

To ensure production of electronic data, counsel should not limit its request to “documents.” Instead, a written request should be prepared to demand production of “electronically stored information.” This can be done most effectively by including the term “electronically stored information” in the request’s definition of “documents.”

The Advisory Committee note on the 2006 amendment to Rule 34(a) indicates that a party’s request for “documents” should logically include electronic data and that a party need not specifically request “electronically stored information.”<sup>144</sup> Notwithstanding this explanation, experience teaches that counsel should specify “electronically stored information” in a request to circumvent the gamesmanship that so often characterizes discovery.<sup>145</sup>

---

<sup>142</sup> *See id.*

<sup>143</sup> *See Williams v. Owens-Illinois, Inc.*, 665 F.2d 918, 933 (9th Cir. 1982) (declining to order production of computer tapes where previously produced wage cards included sought after information); *see also In re Payment Card Interchange Fee and Merch. Disc. Antitrust Litig.*, No. MD 05-1720 (JG) (JO), slip op. at 4 (E.D.N.Y. Jan. 12, 2007), *available at* 2007 WL 121426 (refusing to order plaintiffs to produce metadata corresponding to its previous productions since defendants did not request metadata and did not timely object to plaintiff’s prior production forms); *Williams v. Sprint/United Mgmnt. Co.*, No. 03-2200-JWL-DJW, slip op. at 6–7 (D. Kan. Dec. 12, 2006), *available at* 2006 WL 3691604 (denying plaintiffs’ request for production of e-mail in native format pursuant to Federal Rule of Civil Procedure 34(b)(iii) since plaintiffs previously accepted paper copies of the e-mails); *Phoenix Four, Inc. v. Strategic Res. Corp.*, No. 05 Civ. 4837(HB), 2006 WL 1409413, at \*3, \*9 (S.D.N.Y. May 23, 2006) (plaintiff could not recoup its costs for converting paper documents into an electronically searchable database because defendants initially offered to produce the documents in electronic format and plaintiff declined this offer).

<sup>144</sup> REPORT, *supra* note 114, at app. C-74.

<sup>145</sup> *See Calcor Space Facility, Inc. v. Superior Court*, 53 Cal.App.4th 216, 221, 61 Cal.

2007] PRESERVING AND OBTAINING METADATA

*E. Clarify Whether Court Orders Require Metadata Disclosure*

A common hobgoblin among practitioners is a court order that is silent or ambiguous regarding a party's obligation to produce metadata.<sup>146</sup> Indeed, in *Williams v. Sprint/United Management*, the defendant escaped discovery sanctions despite its misconduct largely due to the "arguable ambiguity" in the court's prior rulings.<sup>147</sup> To remedy such a problem, counsel should request that metadata be produced by the other side in its notice of motion and proposed order. Counsel may also consider asking at oral argument and, if necessary, with further motion practice, whether a party has been ordered specifically to produce metadata. This will help clarify the parties' rights and obligations on the issue.

VI. CONCLUSION

The law governing the preservation and production of metadata remains largely undeveloped. Nevertheless, the case law emerging on this issue provides valuable insight to litigants. The amended Federal Rules also supply much needed guidance about handling this particularly dynamic source of electronic data in litigation. As the amended rules are construed and interpreted, additional case law will further evolve to better guide litigants in their efforts to understand, preserve, and obtain metadata. These changes should lead to better practices with respect to electronically stored information and will ultimately enhance client representation.

---

Rptr. 2d 567, 570 (Cal. Ct. App. 1997) ("We are also aware the discovery process is subject to frequent abuse and, like a cancerous growth, can destroy a meritorious cause or defense. . . . Our observations of the day to day practice of law lead us to conclude this cancer is spreading . . .").

<sup>146</sup> *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640, 656 (D. Kan. 2005).

<sup>147</sup> *Id.* ("This lack of clear law on production of metadata, combined with the arguable ambiguity in the Court's prior rulings, compels the Court to conclude that sanctions are not appropriate here.").