The Columbia
SCIENCE AND TECHNOLOGY LAW REVIEW
www.stlr.org

PRODUCTION, PRESERVATION, AND DISCLOSURE OF METADATA

J. Brian Beckham[*]

As the use of information technology increasingly pervades every facet of our personal and professional life, legal practitioners are taking increasing notice of the effect that metadata can have on their practice. In particular, the prevalence of metadata threatens to have a dramatic effect on discovery issues, such as document retention and production. This article endeavors to define and discuss the concept of metadata, and then explore how this new category of information will apply to traditional notions of waiver and privilege. It will then highlight several proposals for the discoverability of metadata, and will conclude with a discussion of the ethical implications for counsel in dealing with electronically transmitted documents.

I. INTRODUCTION

Recently there has been a significant amount of commentary, both in case law and in scholarly articles, on the topic of electronic discovery. For example, the Southern District of New York only just decided the infamous *Zublake* series of cases,[1] in which the parties were sanctioned because their counsel did not communicate to their respective information technology (IT) directors that they must preserve metadata (i.e., hidden information in electronic documents *about* the document), in the face of pending lawsuits.[2] Most of the discussion to date, however, has focused on discovery issues, such as document production, retention, sanctions, and resulting

[*] The John Marshall Law School, J.D. 2005; LL.M. in Information Technology *with honors* 2005. For additional information, *see* http://www.evolut1on.com (last visited Dec. 1, 2005). *Soli Deo Gloria*.

[1] *Zublake v. UBS Warburg LLC,* 382 F. Supp. 2d 536 (S.D.N.Y. 2005).

[2] *See Zublake v. UBS Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003), where the court summarized the scope of a party's preservation obligation as follows:

> Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a "litigation hold" to ensure the preservation of relevant documents. As a general rule, that litigation hold does not apply to inaccessible backup tapes . . . On the other hand, if backup tapes are accessible . . . then such tapes would likely be subject to the litigation hold.

inferences. In the ABA Journal for April of 2005, Jason Krause wrote about "The Paperless Chase."[3] One e-discovery company mentioned in his article, Evidence Exchange, declares the prominence of this issue on their homepage: "Electronic data has become the crucial source of discoverable evidence in corporate litigation and regulation. This presents many new challenges to which today's companies and their counsel must respond."[4] The legal profession has taken notice of this emerging issue as well. For instance, the Ninth Circuit Advisory Board issued a Proposed Model Local Rule on Electronic Discovery in May of 2004.[5] Among its proposals, the Board suggested that "electronic documents shall be produced in electronic form (including metadata) absent specific objection, agreement of the parties, or order of the court."[6]

The concept of metadata has reared its head with increasing frequency over the past few years. Several infamous examples can serve to illustrate this point. One aspect of metadata is that it may reveal the author(s) and/or editor(s) of electronic documents.[7] For example, in 2000, a democratic candidate for Senate discovered through metadata that several e-mail attachments critical of his campaign were authored by the opposition's chief-of-staff. In another governmental blunder, the British Government released a report on Iraq, which was purportedly based on high-level intelligence and inter-governmental sources. The report turned out to be largely plagiarized from a report on Middle East affairs written by Ibrahim al-Marashi.[8]

Another feature of metadata is that it can reveal information such as edits and changes to electronic documents (similar to Microsoft Word's "Track Changes" feature).[9] In a more recent example, in a suit over the licensing of an early version of IBM "open-source" UNIX code (often known by its popular implementations such as Linux), the SCO Group revealed part of its litigation strategy by alerting the world that its suit against DaimlerChrysler was originally intended for Bank of America, and that the venue of Michigan was eliminated. The SCO Group blundered again by revealing an intra-company e-mail which reveals that there is, in fact, potentially no copyright infringement to be found in several implementations of UNIX (i.e.,

[3] Jason Krause, *The Paperless Chase*, A.B.A. J., Apr. 2005, at 49 (describing some of the pitfalls that awaits for companies unaware of data retention and scouring methods, and explains how traditional discovery methods may prove difficult when applied to data stored electronically).

[4] Evidence Exchange, http://www.evidenceexchange.com/ (last visited Dec. 1, 2005).

[5] Ninth Circuit Advisory Bd., Proposed Model Local Rule on Electronic Discovery, http://www.krollontrack.com/library/9thCirDraft.pdf (May, 2004).

[6] *Id.* at 5.

[7] *See*, *e.g.*, Nadine C. Warner, *Metadata 101: What Lies Beneath*, http://www.abanet.org/govpub/Metadata_excerptsummer04.pdf (last visited Dec. 1, 2005) (explaining that metadata has revealed the author of electronic documents in the past).

[8] Barry Rubin, *British Government Plagiarizes MERIA Journal: Our Response*, Middle East Review of International Affairs, http://meria.idc.ac.il/british-govt-plagiarizes-meria.html (last visited Dec. 1, 2005).

[9] Stephen Shankland & Scott Ard, *Hidden Text Shows SCO Prepped Lawsuit Against BofA*, http://news.com.com/2100-7344_3-5170073.html?tag=nefd_lede (Mar. 4, 2004).

admitting that there is no basis for its heavy-handed tactics against the open-source community).[10]

While there may be some merit to the suggestion that SCO, a tech-savvy group, let the cat out of the bag intentionally, it is just as likely that this was simply a mistake by the company's attorneys. Whether or not it was intentional, the information was revealed. The question remains whether such information is within the proper scope of discovery if it was unintentionally revealed. Currently, there is a strong trend toward treating such unintentionally disclosed metadata as discoverable. Assuming that this is proper, there is some question of the duties of preservation or destruction of metadata. Of even greater significance perhaps, there are questions concerning the extent to which parties may search for metadata.

Forming the backdrop for discovery in federal cases are Federal Rules of Civil Procedure 26 and 34. Rule 26(b)(1) states that "[p]arties may obtain discovery regarding any matter, not privileged, that is relevant to the claim or defense of any party."[11] However, this rule imposes limitations on the manner, scope, and burden of discovery.[12] Rule 34 adds that a party may serve upon another a request for documents "as they are kept in the usual course of business."[13] Section II of this paper will first define and explain the concept of metadata. It will also discuss traditional waiver of privilege as related to inadvertent disclosure of privileged information, and then turn to application of those principles to metadata. While there are no cases thus far directly discussing the disclosure of metadata, two New York State Bar Association Opinions are instructive. Several proposals relating to the discoverability of metadata will be discussed. Section III addresses the ethical implications for counsel, including potential duties to scrub, preserve, and possibly search for metadata in electronically transmitted documents.

II. BACKGROUND

A. *Metadata Explained*

Metadata is often referred to as "data about data."[14] Users of popular word processing software, such as Microsoft Word, may not be aware that when a document is created, the text generated is not the only information that is saved as part of the file, but also that metadata is also included in each document. For an example of this, simply take any Microsoft Word document and save it into a document in plain-text format. Notice that the Microsoft document

[10] *See* CowboyNeal, *Unsealed SCO Email Reveals Linux Code is Clean*, Slashdot.org, http://linux.slashdot.org/article.pl?sid=05/07/14/226208&from=rss (July 14, 2005); *see also* MadScientist, *The Michael Davidson Email/Swartz Memo - SCO v. IBM*, Groklaw.net, http://www.groklaw.net/article.php?story=20050714144923365 (July 14, 2005) (describing the SCO Group's blunder of revealing an intra-company e-mail).

[11] Fed. R. Civ. P. 26.

[12] *See id.*

[13] Fed. R. Civ. P. 34.

[14] Warner, *supra* note 7, at 1.

has a much larger file size. This is due in part to the "added features" of metadata. Microsoft explains the value-added aspects of metadata provided by its software quite well:

> Whenever you create, open, or save a document in Word [], the document may contain content that you may not want to share with others when you distribute the document electronically. This information is known as metadata. Metadata is used for a variety of purposes to enhance the editing, viewing, filing, and retrieval of Microsoft Office documents.
>
> The following are some examples of metadata that may be stored in your documents: Your name, Your initials, Your company or organization name, The name of your computer, The name of the network server or hard disk where you saved the document, Other file properties and summary information, Non-visible portions of embedded OLE objects, The names of previous document authors, Document revisions, Document versions, Template information, Hidden text, Comments
>
> Metadata is created in a variety of ways in Word documents. As a result, there is no single method to remove all such content from your documents.[15]

Microsoft goes on in the same article to explain different methods to eliminate metadata. However, these processes are both time consuming and inefficient. For users of recent versions of Microsoft Office, the program now offers a tool for more swift removal of metadata across multiple documents.[16]

Not to vilify Microsoft, Corel WordPerfect also contains metadata that can be easily uncovered; documents can even be "reverse edited" in Corel.[17] At least with Word documents, the majority of metadata is not ordinarily visible (except, of course, for comments and tracked changes intended to be viewed by collaborators). Nevertheless, with some basic tools that are available online, more deeply hidden metadata may be uncovered.[18]

Metadata is not restricted to document-handling software. As Scott Nagel points out, one of the most important issues surrounding metadata is that it is created when e-mails are sent.[19] E-mail metadata carries the same types of identifying data as do other electronic documents, as

---

[15] *See generally* David Hricik, *The Transmission and Receipt of Invisible Confidential Information*, http://www.hricik.com/eethics/Metadata1103.doc (2003) (citing Microsoft Corp., *How to Minimize Metadata in Word 2002*, http://support.microsoft.com/default.aspx?scid=kb;en-us;290945 (Mar. 3, 2005)).

[16] Microsoft Corp., *Office 2003/XP Add-in: Remove Hidden Data*, http://www.microsoft.com/downloads/details.aspx?FamilyID=144e54ed-d43e-42ca-bc7b-5446d34e5360&displaylang=en (last visited Dec. 1, 2005).

[17] *See*, *e.g.*, Warner, *supra* note 7, at 1.

[18] Ken Colburn, W*ord's Hidden Secret*, http://www.abc15.com/tech/datadr/index2004.asp?did=10252 (last visited Dec. 1, 2005).

[19] Scott Nagel, *Embedded Information in Electronic Documents: Why Metadata Matters* (July, 2004), http://www.abanet.org/lpm/lpt/articles/ftr07044.html.

well as the specific version of a document attached to a particular email. This information can be used to settle disputes over when information was exchanged, the fabrication of documents by interested parties, and the policies and practices of a company.[20] Metadata may even be used for efficient purposes, such as searching for documents by keywords and other criteria.[21] Metadata can also be used to settle billing disputes.[22] In a New York State Bar opinion discussed below, an attorney used e-mail to surreptitiously trace and examine electronic documents.

Despite the potentially negative implications of metadata, it is important to note the possibility of hiding or scrubbing it. One commonly suggested method is to create a portable document file ("PDF"), which is essentially a photocopy of an electronic document viewed as a picture on a users screen. This method, however, requires considerable additional storage space. Other methods include programs such as iScrub from Esquire Innovations,[23] Workshare, and Protect 3.0.[24] The implications and duties of such programs are discussed further below.

B. *Waiver of Privilege: Inadvertent Disclosure*

As a preliminary matter, it must be determined whether a privilege, such as attorney-client or work-product, in fact exists.[25] As documented by Dean Wigmore:

> (1) [w]here legal advice of any kind is sought (2) from a professional legal adviser in his capacity as such, (3) the communications relating to that purpose, (4) made in confidence (5) by the client, (6) are at his instance permanently protected (7) from disclosure by himself or by the legal adviser, (8) except the protection be waived.[26]

Concerning work-product, Fed. R. Civ. P. Rule 26(b)(3) defines it as "the mental impressions, conclusions, opinions, or legal theories of an attorney or other representative of a party

---

[20] *See id.*

[21] *Id.*

[22] The availability of metadata to settle billing disputes brings up another interesting point – the infamous issue of recycled documents and "double-billing" by attorneys. Attorneys should take care in submitting electronic documents to clients as they may easily reveal the amount of time spent (at which billing rate), and the number of people who worked on a document.

[23] *See* Ask the IT Guy, *Scrubbing Metadata & Saving Email*, Modern Practice: Findlaw's Law Practice & Technology Magazine (July, 2003), http://practice.findlaw.com/askitguy-0703.html.

[24] Jim Wagner, *Scrubbing Content Metadata*, Internetnews.com: Enterprise (Aug. 23, 2004), http://www.internetnews.com/ent-news/article.php/3398651. *See also* general information available at http://www.metadatarisk.org (last visited Dec. 1, 2005).

[25] *See* Andrew N. Plasz, *Waiver of Privilege for Documents Inadvertently Disclosed during Discovery*, 93 Ill. B.J. 126 (2005).

[26] *See id. See also United States v. Evans*, 113 F.3d 1457, 1461 (N.D. Ill. 1997) (citing 8 John Henry Wigmore, Evidence in Trials at Common Law § 2292 (John T. McNaughton rev. 1961)).

concerning the litigation."[27] Moreover, the rule provides that a court shall protect against disclosure of an attorney's work-products.[28] Once a court determines that a document is protected by an applicable privilege, the inquiry shifts to whether the disclosure was inadvertent.

In *Maldonado v. New Jersey*, the court noted that generally, a waiver of the attorney-client privilege "must be a knowing and intentional act to be effective."[29] In *Maldonado*, two of the defendants had written a privileged letter to their former attorney, the state's Deputy Attorney General.[30] The letter wound up in the plaintiff's mailbox, who subsequently turned it over to his attorney.[31] There was a dispute over whether any privilege had been waived.[32] The court found that the privilege had not been waived based on the reasonableness of the precautions taken to prevent disclosure, the fact that there was only one arbitrary disclosure, and the risk of prejudice to the defendant.[33] The court noted that as far as privilege was concerned, there are three theories of waiver, reflecting the level of culpability of the attorney.[34]

The first, objective, standard maintains that *any* inadvertent disclosure of a privileged document vitiates the privilege and constitutes an effective waiver,[35] the theory being that one "can't unring a bell." The opposite, subjective, standard holds that since the client holds the privilege and lacks the intent to waive the privilege, any purported waiver by the attorney is ineffective.[36] The court in *Maldonado*, however, adopted a third, balancing view, used by most courts,[37] which seeks to focus on the reasonableness of steps taken to preserve the confidentiality of the privileged documents.[38] The court found the following factors helpful in determining whether there had been such negligence that an inadvertent waiver should be deemed intentional, resulting in a waiver of the privilege attached:

(1) the reasonableness of the precautions taken to prevent inadvertent disclosure in view of the extent of the document production;
(2) the number of inadvertent disclosures [scope of discovery];

---

[27] Fed. R. Civ. P. 26(b)(3).

[28] *Id.*

[29] *Maldonado v. New Jersey*, 225 F.R.D. 120 (D.N.J. 2004).

[30] *Id.*

[31] *Id.* at 125.

[32] *Id.* at 126.

[33] *Id.* at 129-32.

[34] *Id.* at 128.

[35] *Id.* at 128. *See also FDIC v. Singh*, 140 F.R.D. 252 (D. Me. 1992).

[36] *Maldonado*, 225 F.R.D. at 128.

[37] *See* Plasz, *supra* note 25, at 128 (citing *Urban Outfitters, Inc. v. DPIC Cos*., 203 F.R.D. 376 (N.D. Ill. 2001)).

[38] *Maldonado*, 225 F.R.D. at 128.

(3) the extent of the disclosure;
(4) any delay and measures taken to rectify the disclosure; and
(5) whether the overriding interests of justice would or would not be served by relieving the party of its error.[39]

First, the crux of this standard is the reasonableness of precautions taken to avoid disclosure. Of course, the reasonableness of any precautions taken must be called into question when there has indeed been an unintended disclosure.[40] Nonetheless, a feature that the *Maldonado* court considered critical was whether the attorney-client privilege can remain intact despite a one-time, unintentional disclosure of privileged information.[41] Among other factors considered by courts in determining the reasonableness of steps taken to avoid disclosure are the creation of a privilege log, the filing of protective orders to prevent such disclosures, and the general scrupulousness of the attorneys, given the nature of the information exchanged.[42]

Second, the number of disclosures will inevitably depend on the number of information exchanges between parties.[43] As in *Maldonado*, other courts have held that one document inadvertently disclosed in a production order of 750,000 pages was inadvertent and that no waiver had occurred.[44] Still, one disclosure in a production of 4,000 documents has been held inexcusable and the privilege therefore waived.[45] As the volume of information exchanged increases, courts may permit multiple inadvertent disclosures to remain privileged. However, there is evidence that with relatively small document requests (e.g., 4,000 pages), multiple inadvertent disclosures may be impermissible.[46]

Third, as to the extent of the disclosure, the information disclosed in *Maldonado* revealed the defendant's "thought processes and trial strategy."[47] The disclosure was total and complete, so that granting a waiver would unfairly prejudice the disclosing party.[48] Perhaps the lesson to be gleaned from this rationale is that where the opposing party will rely on disclosed documents,

---

[39] *Id.* (citing *Ciba-Geigy Corp. v. Sandoz, Ltd*., 916 F. Supp. 404, 410-11 (D.N.J. 1995)).

[40] *See* Plasz, *supra* note 25, at 129 (citing *Draus v. Healthtrust, Inc*., 172 F.R.D. 384 (S.D. In. 1997)).

[41] *Maldonado*, 225 F.R.D. at 129.

[42] *See* Plasz, *supra* note 25, at 128 n.18.

[43] *Id.* (citing *Parkway Gallery Furniture, Inc. v. Kittinger/Pennsylvania House Group, Inc.*, 116 F.R.D. 46 (M.D.N.C. 1987) (deeming 12,000 documents voluminous); *Harmony Gold U.S.A. v. FASA Corp.*, 169 F.R.D. 113 (N.D. Ill. 1996) (disclosure of one document out of 14,000 held inadvertent)).

[44] *Id.* at 129 (citing *R.J. Reynolds Tobacco Co. v. Premium Tobacco Stores, Inc*., 2001 WL 1571447, at *3 (N.D. Ill 2001)).

[45] *See id.* (citing *Central Die Casting and Mfg. Co, v. Tokheim Corp.,* 1994 WL 444796, at *5 (N.D.Ill 1994)).

[46] *See, e.g., Ciba-Geigy Corp. v. Sandoz, Ltd*., 916 F. Supp. 404, 414 (D.N.J. 1995) (where production involved 681 documents, the disclosure of 23 pages of privileged documents was evidence of carelessness, and as a result, privilege was deemed waived).

[47] *Maldonado v. New Jersey*, 225 F.R.D. 120, 130 (D.N.J. 2004).

[48] *Id.*

such reliance will be allowed, unless there is an obvious duty to return the documents.[49] One problem with the assertion of any ethical obligation to return privileged documents is that there will inevitably be substantial variation in the amount of privileged information actually disclosed (i.e., read by the opposing party), and gauging the extent of disclosure will rely in part on the good faith of the returning party. To this effect, Rule 4.4 of the ABA Model Rules of Professional Conduct states that a "lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender."[50] Whether the returned privileged information will be considered waived is a matter to be resolved by the courts on the merits of each case, based on that jurisdiction's rules of professional conduct.

Fourth, as to the amount of delay between the disclosure and its subsequent discovery, the *Maldonado* court pointed out that this factor can cut both ways.[51] Both parties may know of the disclosure, and hence, any delay may be the result of either party. Courts have held that both six weeks and six months were evidence of negligence on the part of the disclosing party such that the disclosed documents were deemed waived; the disclosing party did not act quickly enough to rectify the disclosure.[52]

Finally, as to the overall fairness to the disclosing party, the court in *Maldonado* held that given the reasonableness of precautions taken to avoid disclosure and the fact that opposing counsel was being disqualified, the interests of justice militated towards a finding of inadvertence, and hence, lack of waiver of the attorney-client privilege with respect to the documents at issue.[53] Not every case will involve attorney disqualification, but the point remains that where reasonable steps were taken to avoid disclosure and inadvertent disclosure of privileged documents occurred nonetheless, justice for the disclosing party will usually outweigh the accidental disclosure. However, where the disclosure is the result of failure to meet a standard of reasonable care, courts will not dispense unlimited forgiveness and waiver of the privilege will be affected. In the end, "the severity of punishment for a mistake should be proportioned to the gravity of the mistake."[54]

---

[49] *See Lifewise Master Funding v. Telebank*, 206 F.R.D. 298, 301-302, 302 n.2. (D. Utah 2002) (Utah imposes an ethical duty not to read documents attorney considers might be privileged and to notify the sender; but it does not accept the ABA opinion requiring return of documents).

[50] Model Rules of Prof'l Conduct R. 4.4 (2003), *available at* http://www.abanet.org/cpr/mrpc/rule_4_4.html; *see also* Diane Karpman, *Unreported Decisions Offer Novel Concepts*, Cal. St. B.J., June 2003, at 23, 23, *available at* http://calbar.ca.gov/state/calbar/cbj.jsp (follow the hyperlinks to Archived Issues, June 2003, Attorney Disciplines, then Ethics Byte) (pointing out that California has adopted the rationale behind Model Rule 4.4).

[51] *Maldonado*, 225 F.R.D. at 130.

[52] *See* Plasz, *supra* note 25, at 129 (citing *Tokar v. City of Chicago*, 1999 WL 138814, at *1 (N.D. Ill. 1999); *Draus v. Healthtrust, Inc.,* 172 F.R.D. 384, 388 (S.D. In. 1997)).

[53] *Id.*

[54] *See* Plasz, *supra* note 25, at 131 (citing *Dellwood Farms v. Cargill, Inc*., 128 F.3d 1122, 1127 (7th Cir. 1997)).

C. *Waiver of Privilege Applied To Metadata*

The standards outlined in cases such as *Maldonado* provide a good analytical framework to apply to inadvertent disclosures, whether they stem from traditional paper exchanges or from electronic document exchanges. The same standards concerning the reasonableness of precautions, number and extent of disclosures, delay, and prejudicial effect[55] are not eliminated simply because the medium has changed. However, the application of these factors to the context of metadata is a question warranting further discussion. Although there is little guidance on this question, two New York State Bar Association Opinions have loosely addressed the matter. One addresses the use of technology to secretly gain an advantage over an opponent, while the other addresses the standard of care warranted when exchanging electronic documents, in order to avoid the undesired disclosure of metadata.

1. New York State Bar Association Opinion 749

New York State Bar Association Opinion 749 – 12/14/01 addresses the use of computer software to surreptitiously examine and trace e-mail and other electronic documents. This opinion suggests that "lawyers may not ethically use available technology to surreptitiously examine and trace e-mail and other electronic documents."[56] Paramount to the Committee on Professional Ethic's (hereinafter "the Committee") reasoning was the fact that using such technology to "get behind" what is visible on a computer screen allows opposing counsel to obtain information relating to the document that the sending party had not intentionally made available to the receiving attorney.[57] The Committee points out that with such technology, lawyers in negotiations may be able to view prior drafts which could reveal settlement figures or interested parties.[58] Even more important to that decision, however, was the ability of attorneys to trace the route of an e-mail exchange, including comments in subsequent e-mails, by placing a "bug" in an e-mail sent to opposing counsel. With such technology, it is possible for the user

[55] The *Maldonado* factors again are:

> (1) the reasonableness of the precautions taken to prevent inadvertent disclosure in view of the extent of the document production;
> (2) the number of inadvertent disclosures [scope of discovery];
> (3) the extent of the disclosure;
> (4) any delay and measures taken to rectify the disclosure; and
> (5) whether the overriding interests of justice would or would not be served by relieving the party of its error.

Maldonado v. New Jersey, 225 F.R.D. 120, 129-30 (D.N.J. 2004).

[56] N.Y. Bar Ass'n Comm. on Prof'l Ethics, Ethics Op. 749 (2001), *available at* http://www.nysba.org/Content/NavigationMenu/Attorney_Resources/Ethics_Opinions/Committee_on_Professional_Ethics_Opinion_749.htm [hereinafter N.Y. Bar Ass'n, Ethics Op. 749].

[57] *Id.*

[58] *Id.*

setting the bug to learn the identity of all senders, and the contents of each e-mail, so long as one person in the chain of e-mails is not using a technological protection against such devices.[59]

The question posed by the Committee was whether lawyers may use such bugging technologies to "surreptitiously examine and trace e-mail *and other electronic documents*."[60] Naturally, the answer reached was no. Not only is this practice an ethical violation, but certain conduct may violate the Electronic Communications Privacy Act of 1986 (ECPA), which is a federal anti-wiretapping statute that makes the ethical inquiry moot.[61] The New York State Committee pointed out that use of such technology allows attorneys to access opposing lawyer's representation, including "confidences and secrets [privileged or confidential information, or work-product]," in violation of the Code of Professional Responsibility.[62] The Committee feared that use of such technology is an unwarranted intrusion on the attorney-client privilege and equated it to soliciting the disclosure of unauthorized communications and exploiting the willingness of others to undermine confidentiality doctrines.[63] Additionally, the Professional Code also prohibits lawyers from engaging in dishonest, fraudulent, or deceitful conduct which is prejudicial to the spirit of justice.[64]

The Committee also examined the intent of the party submitting documents to opposing counsel, although it is not clear what role intent should play in inadvertent disclosure analysis.[65] Perhaps this is because the sending party does not intend his opponent to discover the hidden metadata, whether it stems from documentary notations or from e-mail route tracing. The Committee drew a comparison to ethical duties not to encourage breaking confidences and privileges, and to return information that was inadvertently disclosed.[66] Essentially, the decision turns on the fact that the sending lawyer has not only sent the confidential or privileged information inadvertently, but has also done so unknowingly and unwillingly.[67] For the Committee, the rationales underlying balancing interests exposed in traditional inadvertent disclosure cases are lacking. It noted "[n]o such balance need be struck here because it is a deliberate act by the receiving lawyer, not carelessness on the part of the sending lawyer, that would lead to the disclosure of client confidences and secrets."[68] The Committee closes by

[59] *Id.*

[60] *Id.* (emphasis added).

[61] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

[62] N.Y. Bar Ass'n, Ethics Op. 749, *supra* note 56.

[63] *Id.*

[64] *Id.*

[65] *Maldonado*, 225 F.R.D. at 128 (questioning whether, after the inadvertent disclosure was discovered, the receiving counsel's conduct constituted a "willful and improper design to avoid the rules of discovery and gain an unpermitted advantage in his litigation.") *See also* cases cited in *supra* note 35 and accompanying text.

[66] N.Y. Bar Ass'n, Ethics Op. 749, *supra* note 56.

[67] *Id.*

[68] *Id.*

adding that "the inquiry that has prompted this opinion underscores the need for all lawyers to exercise care in using Internet based e-mail. Accordingly, we reiterate the admonition . . . that 'lawyers must always act reasonably in choosing e-mail for confidential communications, as with any other means of communication.'"[69]

2. New York State Bar Association Opinion 782

The 2001 opinion is reiterated by Opinion 782 – 12/8/04, which poses the question: "DR 4-101(B) states that a lawyer shall not 'knowingly' reveal a confidence or secret of a client. Does a lawyer who transmits documents that contain 'metadata' reflecting client confidences or secrets violate DR 4-101(B)?"[70] Although not directly addressing the question, the opinion concludes that "[l]awyers have a duty under DR 4-101 to use reasonable care when transmitting documents by e-mail to prevent the disclosure of metadata containing client confidences or secrets [which may include keeping up with technological changes in information exchange]."[71] In this opinion, the Committee addresses metadata, not in the sense of e-mail tracing and data capture, but in the sense more commonly known: the data underlying electronic files such as Word documents. The Committee adeptly points out the concerns with inadvertent disclosure of metadata, in that

> [m]etadata may reveal the persons who worked on a document, the name of the organization in which it was created or worked on, information concerning prior versions of the document, recent revisions of the document, and comments inserted in the document in the drafting or editing process. The hidden text may reflect editorial comments, strategy considerations, legal issues raised by the client or the lawyer, legal advice provided by the lawyer, and other information. Not all of this information is a confidence or secret, but it may, in many circumstances, reveal information that is either privileged or the disclosure of which would be detrimental or embarrassing to the client.[72]

The Committee does not add much to the previous warnings that privileged and confidential information may be inadvertently disclosed in the form of metadata, and that as a rule, this is undesirable. Falling back on the reasonableness lynchpin, the Committee reiterates that reasonable care must be used when transmitting or exchanging electronic documents, and that each lawyer must weigh the risks of such exchanges as may be appropriate under the

[69] *Id.* (citing N.Y. Bar Ass'n Comm. on Prof'l Ethics, Ethics Op. 709 (1998), *available at* http://www.nysba.org/Content/NavigationMenu/Attorney_Resources/Ethics_Opinions/Committee_on_Professional_Ethics_Opinion_709.htm)).

[70] N.Y. Bar Ass'n Comm. on Prof'l Ethics, Ethics Op. 782 (2004), *available at* http://www.nysba.org/Content/NavigationMenu/Attorney_Resources/Ethics_Opinions/Opinion_782.htm.

[71] *Id.*

[72] *Id.*

circumstances.[73] Ultimately, the opinion concludes that attorneys must "stay abreast of technological advances and the potential risks in transmission in order to make an appropriate decision with respect to the mode of transmission."[74] The overarching rationale for this conclusion was that since the New York State Bar Association was breaking new ground, so to speak, reasonableness by all parties involved carried the day.

D. *Additional Treatment of Metadata (Ninth Circuit Advisory Board Proposed Model Local Rule on Electronic Discovery)*

Not only do the New York Bar Association opinions point to a duty to avoid inadvertently disclosing metadata by staying technologically informed, but other entities have also addressed the issue. For example, in May of 2004, the Ninth Circuit Advisory Board issued a Proposed Model Local Rule on Electronic Discovery. Among its proposals, the Board suggested that "[e]lectronic documents shall be produced in electronic form (including metadata) absent specific objection, agreement of the parties, or order of the court."[75] Additionally, in August of 2004, the ABA Section of Litigation Electronic Discovery Task Force published its proposed Amendments to the Civil Discovery Standards regarding document production and preservation of documents, which state:

> [t]he duty to produce [electronic information, e.g., e-mail, word processing documents, presentations] may be, but is not necessarily, coextensive with the duty to preserve.
>
> . . .
>
> . . . A party requesting information in electronic form should also consider . . . [a]sking for the production of metadata associated with the responsive data — i.e., ancillary electronic information that relates to ~~relevant~~responsive electronic ~~documents~~data, such as information that would indicate ~~*(a)* whether~~ and when the responsive electronic ~~mail was sent or opened by its recipient(s) or *(b)* whether and when information~~data was created ~~and/or~~, edited, sent, received and/or opened.
>
> . . .
>
> At the initial discovery conference, the parties should confer about any electronic discovery that they anticipate requesting from one another, including . . . [p]reservation of potentially responsive data, specifically

[73] *Id.* (footnote omitted).

[74] *Id.*

[75] Ninth Circuit Advisory Bd., Proposed Model Local Rule on Electronic Discovery, Rule 3, at 5 (May 2004), http://www.krollontrack.com/library/9thCirDraft.pdf.

> addressing . . . metadata reflecting the creation, editing, transmittal, receipt or opening of responsive data.[76]

These proposed amendments reflect the changing nature of electronic discovery both in the abstract and as applied to metadata. While there is currently no case law on point, that is sure to change in the near future, given the rise of electronic document storage and exchange, particularly in corporate and Internet-related litigations.

III. ETHICAL IMPLICATIONS

A. *Does Due Diligence Require Scrubbing or Preserving Metadata?*

Scrubbing electronic documents and communications could be considered akin to a policy of shredding documents. While this may be reasonable under some circumstances, when litigation is anticipated or ongoing, there is a duty to preserve electronic documents in their original form, subject to any privileges or confidences. Privileged and confidential information, such as attorney work-product, may be inadvertently transmitted to opposing counsel during information exchanges. While there is no direct authority on point, the NYSBA opinions, ethical cannons of all state bar associations, and common sense dictate that reasonable care must be used in guarding electronic information exchanges. Whether reasonableness currently requires employing a scrubber such as the Microsoft removal tool, iScrub, Workshare, Protect 3.0, or using PDF format remains an open question. Certainly there is no harm in using such tools, and prudence would dictate that, since they are available at relatively low cost in comparison to the potential damage of disclosing a confidence, privilege, or work-product, attorneys should use them regularly. The alternative is simply to hope that no damaging metadata is passed during an exchange of information and that opposing counsel will not discover it even if it is. While this may be a valid assumption at present, the question remains of how future technological advances, which undoubtedly will make it easier to scrub and search for metadata, will affect that assumption.

As a corollary to any duty to scrub metadata, in certain situations there is a duty to preserve metadata. This preservation duty will vary with context, but will be present at least when opposing counsel has served notice of need for any metadata under applicable civil procedure rules (e.g., Rules 26 and 34 in the federal context). Failing to preserve metadata where circumstances dictate preservation may be sanctionable and may result in adverse inferences against the deleting party.[77] In such instances, metadata may reveal the date a certain fact was known, which is crucial in tort and product liability actions. Metadata may also serve to protect a party where forging of documents could be proven through metadata. The flipside of preservation is automatic scrubbing, which may be possible with available tools. However, the

[76] A.B.A., Amendments to Civil Discovery Standards, §§ 10, 29(b)(ii), 31(a), http://www.abanet.org/litigation/taskforces/electronic/ (follow "Final Revised Standards" hyperlink) (Aug. 2004) (proposed amendments are underlined or stricken through).

[77] *Zublake v. UBS Warburg LLC,* 382 F. Supp. 2d 536, 546 (S.D.N.Y. 2005) (note that the court did not allow adverse inferences against the deleting party in this case, because the evidence of sanctions was inadmissible).

availability of this method will depend upon the stage of litigation (i.e., whether it is used as a general business practice or during discovery).[78]

B. *Does Due Diligence Require Searching for Metadata?*

Searching for metadata is currently only the purview of tech-savvy lawyers. However, eventually it will be the norm. Much like the reduction in fees for electronic filings at the U.S. Patent & Trademark Office, financial factors such as sanctions and liability will compel reluctant lawyers so that searching for metadata becomes commonplace. Underlying the assumption that there is a duty to avoid disclosure of metadata is the premise that there may be parties who will search for it. Realizing this, the question arises as to whether there is ever a duty to search for metadata – something heretofore discussed only in the writings of attorneys speculating on the issue. In addition to the scenarios presented above (i.e., using metadata to prove the date a material fact was known or to prove fraud), metadata can also reveal blind carbon copy (bcc) addressees in e-mails.[79] Whether failing to search for metadata is a violation of a duty to clients is unclear. However, as knowledge of the implications of metadata increases and tools to carry out such searches become more affordable and user-friendly, the duties of due diligence may increasingly require such searches.

---

[78] Dennis Kennedy & George Socha, *Muddling Through the Metadata Morass*, http://www.discoveryresources.org/04_om_electronic_discoverers_0405.html (May 2004).

> If these are your own documents, to be sent out by you in your normal course of business, scrub away. If they are discovery documents, think "scrubbing = shredding." In litigation, this is the "Danger, Will Robinson! Danger!" moment. If you make a unilateral decision to strip files of their metadata and produce the stripped files without even notifying the other side of what you have done, the consequences to you could be dire. If you feel you must strip out the metadata, at least let the other side know what you plan to do first; it might seem as if you are giving up a strategic advantage, but consider this: how do you pronounce "spoliation"? Do you like the sound of "ethics violation"?

[79] For such scenarios, *see*, *e.g.*, Scott Nagel, *Embedded Information in Electronic Documents: Why Metadata Matters*, http://www.abanet.org/lpm/lpt/articles/ftr07044.html (July 2004).

> In one case, a plaintiff claimed that she was discharged in retaliation for making a sexual harassment complaint. To refute the allegation of retaliatory motive, the defendant produced a memo, dated before her sexual harassment complaint, that included the plaintiff on a list of employees to be let go in a planned seasonal layoff. She claimed that the memo was fabricated in response to the litigation. The memo's metadata confirmed its date of creation, prior to her complaint.
>
> Another terminated employee fabricated an e-mail to suggest that a manager with whom she had a romantic relationship had made the decision to terminate her. metadata [sic] exposed the plaintiff herself as the document's author.
>
> Yet another plaintiff contended that the defendant had improperly omitted some e-mails from production. The defendant refuted this claim by reconstructing a chain of e-mails, establishing that it had produced all that was requested.

C. *Two Levels of Culpability under the NYSBA Rationales: Scrubbing and Searching*

There are two lines of thought regarding inadvertent disclosures of metadata, as demonstrated by the fears and rationales espoused by both the commentators and the NYSBA. The first addresses a situation where a party takes reasonable precautions to hide or scrub metadata, while the second addresses a situation where a party neglects to take necessary steps. The apparent tension between these ideas is reconciled by looking at the intent of the parties involved – whether there is intent to deceive, or whether their actions are properly considered diligent.

1. Unauthorized Searching

Where a party purposefully attempts to hide information from the opposition, the steps required to place that party under the protection of reasonableness are found.[80] When a party takes affirmative steps to scrub or convert documents into PDF format to avoid inadvertent disclosure of potentially damaging metadata, it is clear that this will suffice to keep the attorney in the clear, as far as ethical obligations toward their clients are concerned. Where this is the case, opposing attorneys should be prepared to respect the same principles: they should not seek to "surreptitiously go behind," in the words of the NYSBA, the other party's efforts. In such instances, the information, for that reason alone, should not be discoverable. The party searching for the metadata is essentially creating a technological arms race to find the best "scrubber defeater" technology, and this should not be permitted. It serves no purpose except to abdicate the principles underlying the privileges and confidences entrusted to attorneys.

Allowing such a practice would be analogous to allowing opposing counsel access to documents tied to litigation before the producing party has any chance to filter work-product, confidential, and privileged material. Naturally, a party should not be permitted to assert the use of a scrubber to avoid disclosing documents within his or her control, which discovery principles dictate should be disclosed, only those protected under applicable rules. Where a party takes affirmative steps to avoid disclosure, opposing counsel may not use technology to "get behind" the protected document; the data are undiscoverable both technologically and ethically.

2. Inadvertent Disclosure

From the same line of reasoning arise implications where a party neglects to meet the standard of reasonable care in avoiding inadvertent disclosures. As in the traditional context, when a party inadvertently neglects to scrub metadata or hide it from the opposition, the metadata should be discoverable because the opposition only has to do a surface scan of the documents (which in some instances may even be a required duty). Failure to meet the standard of reasonable care should not be rewarded, but this is not to say that it should warrant automatic disclosure because the analysis espoused in *Maldonado* and similar cases should still be followed. In such a case, there is no effort to deceive the producing party into revealing confidential,

[80] *See Maldonado v. New Jersey*, 225 F.R.D. 120, 127 (D.N.J. 2004); *see also* cases cited in *supra* notes 29–35 and accompanying text.

privileged, or work-product materials. The party performing the search is simply using an available tool to expedite the searching process. This practice should not be prohibited; to do so may even be an impediment to the duties of competence and advocacy for the client's best interests.

IV. CONCLUSION

Traditional waiver of privilege standards apply to inadvertent disclosures of privileged metadata. As this article has shown, two New York State Bar Association Opinions are instructive, as is the proposed model rule in the Ninth Circuit. The ethical implications for counsel, including potential duties to scrub, preserve, and possibly search for metadata in electronically transmitted documents may not be commonplace yet, but as time passes, the ramifications of failing to eliminate or search for metadata will likely increase. While the applicable ethical obligations have not yet been fully established, prudence in counseling and document exchange warrants at least learning of the repercussions of metadata disclosure. Jurisdictions other than New York will inevitably address this matter, and are likely to follow the views of the NYSBA since they are based on reasoned application of traditional discovery principles to metadata. Where a party takes affirmative steps to avoid disclosure, the data is undiscoverable and opposing counsel may not use technology to "get behind" the protected document. Similarly, failure to meet the standard of reasonable care should not be rewarded, and while it should not warrant automatic disclosure, the analysis espoused in *Maldonado* and similar cases should be followed. Electronic document exchange and retention is on the rise because this method is simply more efficient in terms of both space-saving and search functionality. Metadata will inevitably be involved in electronic discovery, and its implications will reshape the legal landscape.