Should You Scrub? Can You Mine? The Ethics of Metadata in the Army

Major Brian J. Chapuran[*]

I. Introduction

Metadata is information contained in an electronic document that is not immediately visible to someone viewing the document. Metadata issues can and do frequently arise in the practice of law in the Army. For example, Client *A* visits the legal assistance office to have a separation agreement prepared. The attorney pulls up the last agreement he drafted, saves the new agreement as a new file, and begins work. A few days later, the attorney e-mails Client *A*, attaching the draft separation agreement. Client *A* opens the document and, because metadata is present, Client *A* is able to find the name of Client *B*, for whom the previous separation agreement was drafted. In this example, the previous client was a Soldier in Client *A*'s unit, thus metadata led to a breach of client confidentiality.

Problems involving metadata also arise in the administrative law division. For example, the chief of administrative law drafts an information paper on a sensitive topic. She sends the information paper by e-mail to the other attorneys in the administrative law division for their review and comment. The other attorneys add their comments to the document and e-mail it to the chief. The chief finalizes the information paper. The information paper is later posted on the installation web-site. Unbeknownst to the attorneys, anyone can now download the information paper and view the individual comments made during the drafting process.[1]

These hypothetical scenarios illustrate the dangers of metadata. Metadata can create ethical issues involving confidential information, attorney work-product, and the deliberative process privilege. Confidentiality has been described as "a fundamental aspect of the right of the effective assistance of counsel."[2] It allows the legal community to be effective in helping people solve problems. The concept of confidentiality "not only facilitates the full development of facts essential to proper representation of the client but also encourages people to seek early legal assistance."[3] It is difficult or impossible for attorneys serving as legal assistance attorneys or trial defense counsel to fully advise their clients if they do not have all the facts from each client, including facts that are embarrassing or damaging to the client's legal position. Clients are not likely to disclose such information if they believe the attorney may share it with other people. The duty of confidentiality provides reassurance to the client that certain information will be kept secret and will not be disclosed unless the client authorizes it or in certain circumstances when it is required by law.[4]

The concept of attorney work-product and the related deliberative process privilege[5] are also vital to the legal profession. This concept encourages the free and open discussion of legal issues among attorneys tackling a common problem. An administrative law division cannot render a thorough and well-reasoned opinion without the attorneys in the office discussing the issue openly and honestly. Similarly, a trial counsel may find it difficult to fully assess a case or prepare for trial without the opinions of fellow trial counsel, senior trial counsel, or chief of justice regarding the strengths and weaknesses of the case. These discussions may take place orally, by e-mail, or by adding comments to drafts of documents. The law encourages this free and open discussion by protecting the thoughts and opinions of the attorneys under the doctrines of attorney work-product and deliberative process privilege.

---

[*] Judge Advocate, U.S. Army. Presently assigned as Command Judge Advocate, 3d Sustainment Command (Expeditionary), Fort Knox, Ky. LL.M., 2009, The Judge Advocate Gen.'s Legal Ctr. & Sch., U.S. Army, Charlottesville, Va.; J.D., 2000, Wake Forest University, N.C.; B.A., 1997, Birmingham-Southern College, Ala. Previous assignments include Chief, Operational Law, 3397th Garrison Support Unit, Chattanooga, Tenn., 2006–2008; Trial Counsel, 12th Legal Support Organization, Team 3, High Point, N.C., 2006; Trial Counsel, Fort Benning, Ga., 2003–2004; Group Judge Advocate, 36th Engineer Group, Talil, Iraq, 2003; Trial Counsel, Fort Benning, Ga., 2002–2003; Administrative and Operational Law Attorney, 1st Cavalry Division, Fort Hood, Tex., 2001–2002; Legal Assistance Attorney, 1st Cavalry Division, Fort Hood, Tex., 2001. Member of the bars of North Carolina and Tennessee. This article was submitted in partial completion of the Master of Laws requirements of the 57th Judge Advocate Officer Graduate Course.

[1] In the area of administrative law, ignorance of the dangers of metadata can also lead to problems when posting documents in a Freedom of Information Act (FOIA) Electronic Reading Room or responding electronically to a FOIA request.

[2] ABA Standing Comm. on Ethics and Prof'l Responsibility, Formal Op. 92-368 (1992).

[3] U.S. DEPT. OF ARMY, REG. 27-26, RULES OF PROF'L CONDUCT FOR LAWYERS R. 1.6 cmt. (1 May 1992) [hereinafter AR 27-26].

[4] *Id.* R. 1.6.

[5] 5 U.S.C. 552(b)(5) (2006). Exemption 5 to the Freedom of Information Act allows government agencies to exempt from release to the public "inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency." *Id.* This exemption is commonly referred to at the deliberative process privilege. Unlike attorney work-product, there is no requirement under this exemption that the document be prepared in anticipation of litigation.

The Army lawyer is put in a unique position when it comes to metadata. Army lawyers—Active Duty, Reserve, National Guard, and civilian—are bound by both the Rules for Professional Conduct in Army Regulation (AR) 27-26[6] (Army Rules) and their licensing state's ethical rules.[7] The Army Rules have not been revised since 1992 and therefore do not specifically address metadata.[8] The American Bar Association (ABA) addressed metadata in a 2006 opinion.[9] However, this opinion is based on revisions to the ABA Model Rules[10] made in 2002 which were not adopted by the Army. Only nine jurisdictions have issued ethics opinions on metadata.[11] The Army Judge Advocate General's (JAG) Corps must follow the lead of these jurisdictions and provide guidance to its members on the issue of metadata.

This article defines metadata and how it is created in Microsoft Word. It then discusses the approaches taken by the ABA and the jurisdictions that have issued opinions on metadata.[12] Finally, it offers a proposal for effectively working with metadata in Army legal practice.

II. Metadata 101

Metadata is commonly referred to as "data about data"[13] or "data that provides information about other data."[14] When you view and send a document electronically, you are only seeing, and may think you are only sending, the document visible on the screen. In reality, what is being sent is much more. For example, in terms of paper documents, you believe you are handing over the finished document. What you are really handing over is the entire manila folder containing the work that went into the finished document. The metadata is analogized to the rest of the paperwork in the folder, including the drafts and comments added by other attorneys.[15] A Microsoft Office support document lists the type of information that may be stored in a document as metadata:

> your name, your initials, your company name 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 [Object Linking and Embedding] objects, the names of previous document authors, document revisions, document versions, template information, hidden text, personalized views, comments.[16]

Some of this information is insignificant and its disclosure does not raise serious concerns. Other types of information, however, raise significant issues with confidentiality, attorney work-product, and deliberative process privilege.

Metadata has many important uses. Microsoft states that the purpose of metadata is to "enhance the editing, viewing, filing, and retrieval of documents."[17] In the second hypothetical at the beginning of this article, metadata can be very useful.

---

[6] AR 27-26, *supra* note 3.

[7] *Id.* R. 8.5(f).

[8] AR 27-26, *supra* note 3.

[9] ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442 (2006).

[10] MODEL RULES OF PROF'L CONDUCT (2008).

[11] *See* Ala. State Bar Office of the Gen. Counsel, Op. No. 2007-02 (2007); Ariz. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. 07-03 (2007); Ethics Comm. of the Colo. Bar Assoc., Ethics Op. 119 (2008); D.C. Bar, Op. 341 (2007); Fla. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-2 (2006); Me. Prof'l. Ethics Comm., Op. 196 (2008); Md. State Bar Ass'n Comm. on Ethics, Op. 2007-09 (2007); N.Y. Comm. on Prof'l Ethics, Op. 749 (2001); N.Y. Comm. on Prof'l Ethics, Op. 782 (2004); Pa. Bar Ass'n Comm. on Legal Ethics and Prof'l Responsibility, Formal Op. 2007-500 (2007).

[12] Metadata is implicated in the context of the emerging practice of electronic discovery. In that context, attorneys may be required to preserve metadata and provide it to opposing counsel. That aspect of metadata is beyond the scope of this article and will not be addressed. *See generally* Crystal Thorpe, *Metadata: The Dangers of Metadata Compel Issuing Ethical Duties to "Scrub" and Prohibit the "Mining" of Metadata*, 84 N. DAK. L. REV. 257 (2008); Philip J. Favro, *A New Frontier in Electronic Discovery: Preserving and Obtaining Metadata*, 13 B.U. J. SCI. & TECH. L. 1 (2007).

[13] Gerald J. Hoenig, *Lawyers Beware: Metadata Is There*, 18 PROB. & PROP. 51, 51 (Sept./Oct. 2004).

[14] Merriam-Webster's Online Dictionary, http://www.merriam-webster.com/dictionary/metadata (last visited July 8, 2009). The term metadata is so new that it cannot be found in many hard-copy traditional dictionaries.

[15] David L. Brandon, *The Hidden Perils of Metadata*, LPL ADVISORY (ABA Standing Comm. on Lawyer's Prof'l Liab., Chicago, Ill.), Fall 2006, at 2.

[16] Microsoft Office Online: Find and Remove Metadata (Hidden Information) in Your Legal Documents, http://office.microsoft.com/en-us/help/HA010776461033.aspx (last visited July 8, 2009).

[17] *Id.*

When several attorneys within a military legal office collaborate on a document, metadata, such as added comments and tracked changes, aids that collaborative process. In the context of military justice, metadata can be useful when trial counsel and defense counsel are working to reach an agreement on a stipulation of fact. As both parties make changes, they may use the track changes feature, then e-mail the changed version to the other party, thus allowing the opposing counsel to see each iteration of changes.

Microsoft Word, the primary word processing software used by the Army JAG Corps, stores metadata in a variety of ways. One well-known example is a file's Properties. The "Properties" window may be opened by right-clicking on the file name and selecting Properties from the drop-down menu. A file's properties is the most general example of metadata in a Microsoft Word document. In the Properties window, the viewer is able to determine the document's author and creation date, among other information. This metadata may initially seem innocuous, but it could become more significant later in a case.[18]

In addition to the properties of a file, Microsoft Word also creates metadata through the use of several other functions. "Track Changes" is a useful way for multiple attorneys, or an attorney and support staff, to ensure that edits are incorporated into a document. All of the succeeding changes, however, are stored with the file as metadata. Another useful feature of Microsoft Word is "Fast Saves." Fast Saves "reduces the chance of losing changes to a document" and is useful in the event of hardware failure.[19] Like Track Changes, when Fast Saves is enabled, "deleted information remains hidden within the document."[20] In addition, the "Comments" feature of Microsoft Word allows multiple users to insert comments into a document. Even if those comments are not visible on a final e-mailed document draft, those comments are still embedded in the file as metadata.[21] Functions such as Fast Save, Track Changes, and Comments are all useful to the creator of Microsoft Word documents. However, the additional information saved, changed or added as a comment is all stored with the file and sent to the recipient when a file is e-mailed.

III. Should You Scrub? Current Approaches—Sender

The ethical implications created by the presence of metadata can be divided into two categories: the obligations of an attorney sending electronic documents and the limitations on the attorney receiving electronic documents.[22] The Model Rules and most jurisdictions require an attorney to take reasonable steps to protect confidential information obtained from their clients.[23] The question then becomes whether that requirement to take reasonable steps creates an obligation to remove metadata, often referred to as "scrubbing" a document,[24] anytime a document is sent?

The ABA has not issued a formal opinion regarding the obligations of attorneys to scrub documents for metadata before sending them. However, under the Model Rules' requirement to take reasonable steps to protect confidential information, such a duty could be inferred. Several jurisdictions have specifically addressed the sending attorney's duties in the context of metadata.[25] All of these jurisdictions come to the same conclusion—an attorney has a duty to take reasonable steps to ensure that metadata is removed. What remains unclear from reading the opinions is what constitutes "reasonable steps." The opinions generally state that what is reasonable will vary with the circumstances.[26]

---

[18] An example of this problem would be if a chief of military justice sat second-chair in a court-martial and later authored the Staff Judge Advocate Recommendation (SJAR). If the SJAR is e-mailed to the defense counsel, metadata would allow him to discover the author of the SJAR. *See* MANUAL FOR COURTS-MARTIAL, UNITED STATES, R.C.M. 1106(b) (2008).

[19] Toby Brown, *Special Handling: How Paper and Electronic Files Differ*, GPSOLO (ABA General Practice, Solo & Small Firm Division, Chicago, Ill.), Sept. 2004, at 23.

[20] *Id.*

[21] David Hricik, *I Can Tell When You're Telling Lies: Ethics and Embedded Confidential Information*, 30 J. LEGAL PROF. 79, 86 (2005/2006).

[22] *See* discussion *infra* Part IV.

[23] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 17 (2008).

[24] *See generally* Campbell C. Steele, *Attorneys Beware: Metadata's Impact on Privilege, Work Product, and the Ethical Rules*, 35 U. MEM. L. REV. 911 (2005); Thorpe, *supra* note 11.

[25] *See, e.g.*, Ala. State Bar Office of the Gen. Counsel, Op. 2007-02 (2007); Ariz. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. 07-03 (2007); Ethics Comm. of the Colo. Bar. Assoc., Ethics Op. 119 (2008); D.C. Bar Legal Ethics Comm., Op. 341 (2007); Me. Prof'l Ethics Comm., Op. 196 (2008); Md. State Bar Ass'n Comm. on Ethics, Op. 2007-09 (2007); N.Y. Comm. on Prof'l Ethics, Op. 782 (2004).

[26] *See, e.g.*, N.Y. Comm. on Prof'l Ethics, Op. 782.

The majority of the opinions addressing the sender's duties set out factors to consider when determining what is reasonable. Alabama set out the following factors: "steps taken by the attorney to prevent the disclosure of metadata, the nature and scope of the metadata revealed, the subject matter of the document, and the intended recipient."[27] Arizona's opinion contains a similar list of factors to consider: "the sensitivity of the information, the potential consequences of its inadvertent disclosure, whether further disclosure is restricted by statute, protective order, or confidentiality agreement, and any special instructions given by the client."[28] New York provides a list of factors:

> the subject matter of the document, whether the document was based on a template used in another matter for another client, whether there have been multiple drafts of the document with comments from multiple sources, whether the client has commented on the document, and the identity of the intended recipients of the document.[29]

Arizona includes as a factor to consider: "any special instructions given by the client."[30] The Arizona opinion goes on to specifically address government lawyers and states that these special instructions "might include the client's informed consent to forego, for financial or other reasons, the acquisition or use of software that is designed to remove metadata . . . ."[31] Based on this language, an Army lawyer licensed in Arizona might be safe not using scrubbing software if there is evidence provided that the Army JAG Corps had considered such software and made an informed decision not to purchase it.

Arizona's opinion is unique in that it goes so far as to say that templates[32] should not be used because of the concern with metadata.[33] Specifically, the opinion states that, "[a] lawyer who prepares a pleading, contract, or other document should use a 'clean' form and not a document that was used for another client."[34] No other jurisdiction has issued an opinion on metadata that includes this caution to refrain from using templates. Given the routine use of templates in the Army, Army lawyers licensed in Arizona should pay special attention to this provision.

Colorado's recent opinion goes even further to impose an obligation on supervisory attorneys. The opinion states that supervisory attorneys have a "duty to make reasonable efforts to make sure that the lawyer's firm has appropriate technology systems in place so that subordinate lawyers and non-lawyer assistants can control the transmission of metadata."[35] Under this rule, an Army lawyer who serves as a Chief of Legal Assistance, for example, would have an obligation to put a policy in place to minimize the risk of inadvertent disclosure through metadata. The jurisdictions addressing metadata all agree that the sender must take "reasonable steps" to protect confidential information. They vary in what factors are used to determine whether the sender has taken "reasonable steps" and some set out additional obligations beyond just taking "reasonable steps."

IV. Can You Mine? Current Approaches—Receiver

Unlike the ethics opinions dealing with the obligations of the sender, no consensus exists among the opinions addressing the obligations of an attorney who receives a document containing metadata. What, if any, constraints a state places on the receiver of an e-mailed document turns on the answers to two questions. First, was the inclusion of the metadata

---

[27] Ala. State Bar Office of the Gen. Counsel, Op. 2007-02.

[28] Ariz. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. 07-03.

[29] N.Y. Comm. on Prof'l Ethics, Op. 782.

[30] Ariz. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. 07-03.

[31] *Id.*

[32] A template is a document type in Microsoft Word that creates a copy of itself each time it is opened. Microsoft Office Online: Create a New Template, http://office.microsoft.com/en-us/word/HA100307541033.aspx (last visited July 18, 2009). This allows information that will remain the same to be used on multiple documents. It also commonly refers to a previously drafted document which can be reused by changing certain information for a new client.

[33] Ariz. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. 07-03.

[34] *Id.*

[35] Ethics Comm. of the Colo. Bar. Ass'n, Ethics Op. 119 (2008).

"inadvertent," thus implicating Model Rule 4.4(b),[36] or its state equivalent? Second, does mining for metadata involve deceit or dishonesty implicating Model Rule 8.4(c),[37] or its state equivalent?

A. Mine, Baby, Mine

1. The American Bar Association

The ABA addressed the issue of how to handle metadata in a formal opinion released in 2006.[38] Before analyzing this ABA Opinion on metadata, this paper will briefly review of the history of inadvertent disclosure of confidential information under the ABA Model Rules. Prior to the 2002 amendments to the Model Rules, no Rule 4.4(b) existed, and thus, nothing that specifically addressed a situation where an attorney inadvertently discloses confidential information.[39] In 1992, the ABA released Formal Opinion 92-368 addressing inadvertent disclosure of confidential material under the then-existing Model Rules.[40] The ABA analyzed the situation by considering the importance of the concept of confidentiality, and whether any more important principle would support a rule allowing a receiving attorney to use inadvertently disclosed confidential material.[41] The ABA considered such principles as deterring or punishing carelessness on the part of the sending attorney, encouraging more care on the part of the sending attorney, as well as enforcing the obligation of the receiving attorney to zealously represent his client.[42] The ABA reached the conclusion that none of these principles were important enough to outweigh the fundamental concept of confidentiality.[43] The result was an opinion that the attorney who receives inadvertently sent confidential information must "avoid reviewing the materials, notify sending counsel if sending counsel remains ignorant of the problem and abide by sending counsel's direction as to how to treat the disposition of the confidential materials."[44]

In 2002, the ABA amended the Model Rules and by adding Rule 4.4(b), addressing inadvertent disclosure of materials.[45] Model Rule 4.4(b) is broader than Formal Opinion 92-368 because "it covers all inadvertent transmissions, not just those which involve confidential information."[46] However, the new rule is also narrower in that "the only obligation imposed . . . is notice."[47] Rule 4.4(b) does not require the receiving attorney to refrain from reviewing or using the inadvertently disclosed material.

In its 2006 opinion on metadata, the ABA found that Model Rule 4.4(b) is "the most closely applicable rule" to the situation involving disclosure of information in metadata.[48] Addressing the first relevant question regarding metadata, the ABA concluded that even if the disclosure of metadata were considered inadvertent, "Rule 4.4(b) is silent as to the ethical propriety of a lawyer's review or use of such information."[49] With respect to the second relevant question regarding metadata, whether mining for it involves deceit or dishonesty, the ABA opinion provides no analysis. Instead, the opinion merely states the conclusion that a lawyer mining for metadata would not violate either Model Rule 8.4(c) (prohibiting deceit

---

[36] MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2008) ("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.").

[37] *Id.* R. 8.4(c) (stating it is professional misconduct for a lawyer to "engage in conduct involving dishonesty, fraud, deceit, or misrepresentation").

[38] ABA Standing Comm. on Ethics and Prof'l Resp., Formal Op. 06-442 (2006).

[39] MODEL RULES OF PROF'L CONDUCT R. 4.4 (2001). The Army has not adopted the 2002 amendments to the Model Rules, and Army Rule 4.4 remains unchanged.

[40] ABA Standing Comm. on Ethics and Prof'l Resp., Formal Op. 92-368 (1992).

[41] *Id.*

[42] *Id.*

[43] *Id.*

[44] *Id.*

[45] MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2008).

[46] David Hricik, *Mining for Embedded Data: Is It Ethical to Take Advantage of Other People's Failures?*, 8 N.C. J.L. & TECH. 231, 237 (2007).

[47] *Id.*

[48] ABA Standing Comm. on Ethics and Prof'l Resp., Formal Op. 06-442 (2006).

[49] *Id.*

or dishonesty) or 8.4(d) (prohibiting conduct prejudicial to the administration of justice).[50] The ABA concluded, therefore, that it is not a violation of the Model Rules to mine for metadata.[51]

2. Maryland

Like the ABA, the State of Maryland reached the conclusion that mining for metadata does not violate its ethical rules.[52] However, Maryland's rules, like AR 27-26, have not been amended to add Model Rule 4.4(b) dealing with the inadvertent receipt of information.[53] The Maryland opinion is based on the fact that their rules impose no obligation on an attorney who receives inadvertently sent confidential information.[54] Since the receiving attorney is under no obligation to even notify the sender that he has received confidential information, the receiving attorney is not prohibited from reviewing and using the information. The Maryland opinion fails to address the argument that mining is deceitful or dishonest and therefore violates Maryland Rule 8.4(c).[55] Maryland attorneys, therefore, are free to mine for metadata and use whatever information they find, even if it is confidential or attorney work-product.

3. Colorado

In May 2008, the State of Colorado addressed the issue of metadata when it released Formal Opinion 119.[56] This opinion states that if an attorney "knows or reasonably should know that a Sending Lawyer (or non-lawyer) has transmitted metadata that contain Confidential Information, the Receiving Lawyer should assume that the Confidential Information was transmitted inadvertently."[57] Accordingly, Colorado Rule 4.4(b) dictates the receiver's obligations.[58] Similar to Model Rule 4.4(b), Colorado's Rule 4.4(b) simply requires the receiving attorney to notify the sending attorney.[59] Colorado's Rule 4.4(b) does not prohibit the receiving attorney from continuing to review the information or using it, even if it is confidential.[60]

Colorado concluded that "there is nothing inherently deceitful or surreptitious about searching for metadata."[61] This conclusion stems from the ease of finding some metadata, therefore it is "misleading" to consider looking for it as"mining."[62] As a result, Colorado does not analyze the possibility of mining for metadata as deceitful or dishonest and therefore possibly in violation of Rule 8.4.

B. No Mining Allowed

Five states have disagreed with the ABA and have explicitly prohibited mining for metadata.[63] Florida and Arizona deal with the problem primarily from the standpoint of inadvertently sent documents. New York, Alabama, and Maine, however, base their prohibition primarily on the view that mining is dishonest and deceitful.

---

[50] *Id.*

[51] *Id.*

[52] Md. State Bar Ass'n Comm. on Ethics, Op. 2007-09 (2007).

[53] MD. LAWYER'S RULES OF PROF'L CONDUCT R. 4.4 (2007).

[54] Md. State Bar Ass'n Comm. on Ethics, Op. 2007-09 (2007).

[55] MD. LAWYER'S RULES OF PROF'L CONDUCT R. 8.4(c) (2007).

[56] Ethics Comm. of the Colo. Bar Ass'n, Ethics Op. 119 (2008).

[57] *Id.*

[58] COLO. RULES OF PROF'L CONDUCT R. 4.4(b) (2008).

[59] *Id.*

[60] *Id.*

[61] *Id.*

[62] *Id.*

[63] *See* Ala. State Bar Office of the Gen. Counsel, Op. 2007-02 (2007); Ariz. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. 07-03 (2007); Me. Prof'l Ethics Comm., Op. 196 (2008); N.Y. Comm. on Prof'l Ethics, Op. 749 (2001); Fla. State Bar Ass'n Comm. on Ethics, Op. 2007-09 (2007).

1. It Was Inadvertently Sent—Florida and Arizona

Chronologically, Florida was the second licensing authority to issue an opinion on metadata, releasing it in 2006.[64] Florida came to the same conclusion as the state of New York—mining is prohibited[65]—but Florida's legal reasoning was substantially different. Florida approached the issue from the perspective of inadvertently sent documents and relied on its own version of Rule 4.4(b).[66] Florida took the position that any confidential information contained in metadata is to be considered as inadvertently sent by the other attorney.[67] Based on this assumption, Florida concluded that a receiving lawyer is prohibited from trying "to obtain from metadata information relating to the representation of the sender's client that the recipient knows or should know is not intended for the recipient."[68]

Although it arguably reached the correct result, Florida's reasoning is flawed. Florida's Rule 4.4(b) is the same as the Model Rule 4.4(b) in that it requires the receiving attorney to simply notify the sender of the inadvertently sent information.[69] Florida's Rule 4.4(b) does not require the receiving attorney to refrain from viewing or using the information, however.[70] Florida's opinion was released just over one month after the ABA interpreted the same rule and reached a different conclusion. This timing raises the question whether Florida considered mining for metadata deceitful and dishonest, but chose not analyze it under Rule 8.4(c).

Arizona's opinion was released in 2007 and also prohibits mining for metadata.[71] Arizona briefly mentioned the premise that lawyers "should refrain from conduct that amounts to an unjustified intrusion into the client-lawyer relationship."[72] In making this assertion, the opinion cited Arizona Ethical Rules 8.4(a)–(d).[73] These rules are similar to Model Rule 8.4(a)–(d) and prohibit, among other things, conduct that involves deceit and dishonesty.[74] However, Arizona did not base its opinion on this reasoning. Arizona went on to discuss the duties of a lawyer who receives a document that is inadvertently sent.[75] The opinion concluded that "if the document as sent contains metadata that reveals confidential or privileged information, it was not sent in the form in which it was intended to be sent."[76] Accordingly, Arizona Ethical Rule 4.4(b),[77] dealing with inadvertently received documents, is applicable. Arizona's version of Rule 4.4(b) goes further than Model Rule 4.4(b)[78] in that it does not require the receiving attorney solely to notify the sender, it also requires the receiving attorney to "maintain the status quo."[79] While not stated expressly, "maintaining the status quo"[80] presumably would prohibit a receiving attorney from reviewing or otherwise using the confidential information contained in the metadata.

---

[64] Fla. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-2 (2006).

[65] *Id.*

[66] *Id.*

[67] *Id.*

[68] *Id.*

[69] *Compare* FLA. RULES OF PROF'L CONDUCT R. 4.4(b) (2006), *with* MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2008).

[70] FLA. RULES OF PROF'L CONDUCT R. 4.4(b) (2006).

[71] Ariz. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. 07-03 (2007).

[72] *Id.*

[73] ARIZ. RULES OF PROF'L CONDUCT R. 8.4(a)-(d) (2004).

[74] *Compare id.*, *with* MODEL RULES OF PROF'L CONDUCT R. 8.4(a)-(d).

[75] Ariz. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. 07-03.

[76] *Id.*; *see also* Hricik, *supra* note 46 (analyzing whether metadata is actually inadvertently disclosed when the sender intended to send the document).

[77] ARIZ. RULES OF PROF'L CONDUCT R. 4.4(b).

[78] *Compare id.*, *with* MODEL RULES OF PROF'L CONDUCT R. 4.4(b).

[79] Ariz. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. 07-03.

[80] ARIZ. RULES OF PROF'L CONDUCT R. 4.4(b).

2. It Is Dishonest and Deceitful—New York, Alabama, and Maine[81]

New York, the first jurisdiction to tackle the issue of metadata, released its opinion on the subject in 2001,[82] prior to the ABA opinion. New York concluded that "the use of computer technology in the manner described above [mining for metadata] constitutes an impermissible intrusion on the attorney-client relationship in violation of the Code."[83] New York opined that mining for metadata violated Disciplinary Rule 1-102(a)(4), which prohibits a lawyer from "[e]ngaging in conduct involving dishonesty, fraud, deceit, or misrepresentation."[84] This New York Disciplinary Rule is identical to Model Rule 8.4(c)[85] and Army Rule 8.4(c).[86] New York went further than just addressing metadata that contains confidential information. The opinion also stated that mining for metadata that may be protected by "the work-product doctrine or that may otherwise constitute a 'secret' of another lawyer's client would violate the letter and spirit of these *Disciplinary Rules*."[87] New York's opinion emphasized the "strong public policy in favor of preserving confidentiality as the foundation of the lawyer-client relationship."[88] New York concluded that protecting confidentiality was a justified restraint on the "uncontrolled advocacy"[89] of zealous representation.

While New York based its opinion primarily on the conclusion that mining for metadata involves deceit and dishonesty, it also raised the issue of inadvertent disclosure of confidential information.[90] New York's opinion was released prior to the amendments to the Model Rules that added the current Model Rule 4.4(b).[91] New York instead looked to the 1992 ABA Opinion 92-368 addressing inadvertent disclosure.[92] Opinion 92-368 concluded that under the earlier version of the Model Rules, a lawyer who receives inadvertently sent confidential materials should not only notify the sender but also should refrain from examining the materials and abide by the sending lawyer's instructions regarding the material's disposition.[93] Because the current Army Rules virtually mirror the rules the ABA interpreted in Opinion 92-368,[94] New York's opinion is useful to an analysis of metadata under the current Army Rules.

While other jurisdictions have followed New York's lead in addressing the issue, Alabama and, more recently, Maine are the only states to adopt similar reasoning. Alabama's opinion, released in 2007, concluded that "the receiving lawyer also has an obligation to refrain from mining an electronic document."[95] The foundation for Alabama's opinion, like New York's, is that mining for metadata involves conduct that is deceitful or dishonest.[96] Alabama states that "mining metadata constitutes a knowing and deliberate attempt by the recipient attorney to acquire confidential and privileged information in order to obtain an unfair advantage against an opposing party."[97]

Maine, the most recent state to address metadata, released Opinion 196 in October 2008.[98] Maine, like Alabama and New York, concluded that mining for metadata is unethical because it is dishonest.[99] Accordingly, the opinion is based on

---

[81] North Carolina has released a proposed opinion that follows this rationale and may be next to join this group. *See* N.C. State Bar Ethics Comm., Proposed 2009 Formal Ethics Op. 1 (2009).

[82] N.Y. Comm. on Prof'l Ethics, Op. 749 (2001).

[83] *Id.*

[84] N.Y. LAWYER'S CODE OF PROF'L RESPONSIBILITY D.R. 1-102(a)(4) (2002).

[85] MODEL RULES OF PROF'L CONDUCT R. 8.4(c) (2008).

[86] AR 27-26, *supra* note 3, R. 8.4(c).

[87] N.Y. Comm. on Prof'l Ethics, Op. 749.

[88] *Id.*

[89] *Id.*

[90] *Id.*

[91] MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2008).

[92] ABA Standing Comm. on Ethics and Prof'l Responsibility, Formal Op. 92-368 (1992).

[93] *Id.*

[94] *Id.*

[95] Ala. State Bar Office of the Gen. Counsel, Op. 2007-02 (2007).

[96] *Id.*

[97] *Id.*

[98] Me. Prof'l Ethics Comm., Op. 196 (2008).

Maine's version of Model Rule 8.4(c).[100] Maine went further to conclude that metadata mining is prejudicial to the administration of justice because it "strikes at the foundational principles that protect attorney-client confidences."[101]

The flaw in an opinion based solely on Model Rule 8.4(c),[102] like Alabama's[103] and Maine's,[104] is that it does not address the problem of the accidental discovery of metadata.[105] In some cases, the receiving attorney may not be actively mining for metadata, but may still discover some. For example, consider an attorney who receives a document from opposing counsel and decides to insert comments into the document before sending it to his partner. When the attorney inserts comments, he may uncover hidden, unintentionally sent comments inserted by the sending attorney.[106] This metadata could reveal confidential information or work-product. However, the receiving attorney accidentally discovered the metadata and was not engaging in conduct that could be considered dishonest or deceitful. An opinion that relies solely on Model Rule 8.4(c)[107] fails to adequately address this situation. The failure to provide adequate guidance in these opinions results in a gap in the protection for confidential information which is inadvertently disclosed in metadata and accidentally discovered.

C. Pennsylvania: The Golden Rule Opinion

Pennsylvania issued an opinion on metadata in 2007.[108] Unfortunately, Pennsylvania's opinion does not provide clear guidance and can best be described as "The Golden Rule[109] Opinion." Pennsylvania's rules include a Rule 4.4(b)[110] dealing with receipt of inadvertently sent documents that is identical to the Model Rule.[111] The Pennsylvania opinion seems to treat all metadata as inadvertently sent.[112] However, it also states that none of Pennsylvania's current rules apply to metadata and fails to apply Rule 4.4(b).[113] Instead, the majority of Pennsylvania's opinion discusses the approaches taken by other jurisdictions.[114] The opinion concludes that it would be too difficult to come up with a rule applicable to all situations.[115] Instead, Pennsylvania leaves the decision of whether to mine for metadata up to each individual attorney.[116] The Pennsylvania Bar Association Committee provides factors Pennsylvania attorneys should consider in deciding whether to mine for metadata.[117] These factors include reciprocity and professional courtesy.[118] This leads to the description of Pennsylvania's approach as "The Golden Rule Opinion"—don't mine for metadata if you don't want others mining for yours.

---

[99] *Id.*

[100] *See* ME. CODE OF PROF'L CONDUCT R. 3.2(f)(3) (2009).

[101] Me. Prof'l Ethics Comm., Op. 196 (2008).

[102] MODEL RULES OF PROF'L CONDUCT R. 8.4(c) (2008).

[103] Ala. State Bar Office of the Gen. Counsel, Op. 2007-02 (2007).

[104] Me. Prof'l Ethics Comm., Op. 196.

[105] *See* Bradley H. Leiber, *Applying Ethics Rules to Rapidly Changing Technology: The D.C. Bar's Approach to Metadata*, 21 GEO. J. LEGAL ETHICS 893, 901 (2008); Ariz. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. 07-03 (2007).

[106] *See* Leiber, *supra* note 105, at 901.

[107] MODEL RULES OF PROF'L CONDUCT R. 8.4(c).

[108] Pa. Bar Assoc. Comm. on Legal Ethics and Prof'l Resp., Op. 2007-500 (2007).

[109] "Do to others as you would like them to do to you." *Luke* 6:31 (New Living Translation).

[110] PA. DISCIPLINARY RULES OF PROF'L CONDUCT R. 4.4(b) (2002).

[111] MODEL RULES OF PROF'L CONDUCT R. 4.4(b).

[112] Pa. Bar Assoc. Comm. on Legal Ethics and Prof'l Resp., Op. 2007-500.

[113] *Id.*

[114] *Id.*

[115] *Id.*

[116] *Id.*

[117] *Id.*

[118] *Id.*

D. A Middle Ground? The District of Columbia Weighs In

The District of Columbia (D.C.) issued an opinion on metadata in 2007[119] that appears to be an attempt to reach a middle ground on the issue.[120] The D.C. opinion requires the receiving attorney to notify the sender and to abide by the sender's instructions "when a receiving lawyer has actual knowledge that the sender inadvertently included metadata in an electronic document."[121] Rule 4.4(b) in D.C. applies to situations where an attorney "knows, before examining the writing, that it has been inadvertently sent."[122] This is unusual, compared with other jurisdictions, in requiring actual knowledge under Rule 4.4(b). Model Rule 4.4(b) sets out a broader rule, applying when the receiver "knows or should know."[123]

The D.C. opinion raises the question of when a receiving attorney will have actual knowledge that material was sent inadvertently and provides two examples. The first scenario occurs when the sender tells the receiver before the receiver reviews the document.[124] The second occurs "when a receiving lawyer immediately notices upon review of the metadata that it is clear that protected information was unintentionally included."[125] This second situation illustrates a "should have known" standard, which D.C.'s Rule 4.4(b) does not contain.[126] In either of these situations, the receiving attorney must notify the sender and abide by his instructions on the disposition of the material.[127] The D.C. opinion does not address the issue of whether active mining for metadata violates Rule 8.4(c) by involving deceit or dishonesty. Thus, the D.C. opinion appears to allow active mining, since it is unlikely the receiver would have actual knowledge of the inadvertent disclosure of material prior to mining for metadata. However, a footnote in the opinion states that the D.C. Bar "does not condone a situation in which a lawyer employs a system to mine all incoming electronic documents."[128] The D.C. Bar could have relied on Rules 8.4 and 4.4(b) and established a clear prohibition on mining for metadata. Instead, they attempted to reach a middle ground, resulting in an opinion that is "somewhat circular and difficult to decipher."[129]

E. The Other Jurisdictions

In the jurisdictions that have not addressed metadata, attorneys must look to existing rules and ethics opinions for guidance. Most jurisdictions that have addressed metadata approach it from the perspective of inadvertent disclosure of information.[130] Although not directly on point, the body of law addressing inadvertent disclosure is arguably applicable to metadata and is relied upon by jurisdictions that have addressed metadata.[131] While the sending attorney did not inadvertently disclose the document, the metadata was inadvertently disclosed.[132] If a jurisdiction has not released an opinion on metadata, an attorney should look to his jurisdiction's treatment of inadvertent disclosure of information.

Jurisdictions generally fall into four categories regarding inadvertent disclosure of information. The first are those that have adopted Model Rule 4.4(b).[133] These jurisdictions impose an obligation on the receiving attorney to notify the sender of

---

[119] D.C. Bar Legal Ethics Comm., Op. 341 (2007).

[120] Leiber, *supra* note 105, at 905.

[121] D.C. Bar Legal Ethics Comm. Op. 341.

[122] D.C. RULES OF PROF'L CONDUCT R. 4.4(b) (2002).

[123] MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2008).

[124] D.C. Bar Legal Ethics Comm. Op. 341.

[125] *Id.*

[126] D.C. RULES OF PROF'L CONDUCT R. 4.4(b).

[127] D.C. Bar Legal Ethics Comm. Op. 341.

[128] *Id.*

[129] Leiber, *supra* note 105, at 907.

[130] *See* discussion *infra* Part IV. *But see* N.C. State Bar Ethics Comm., Proposed 2009 Formal Ethics Op. 1 (2009) (taking the position that Rule 4.4(b) is not applicable because it applies to writings that were never intended for the receiving attorney).

[131] *See* discussion *infra* Parts IV.A, IV.B, IV.D.

[132] Hricik, *supra* note 21, at 99.

[133] Andrew M. Perlman, *Untangling Ethics Theory from Attorney Conduct Rules: The Case of Inadvertent Disclosures*, 13 GEO. MASON L. REV. 767, 783 (2006).

the inadvertently disclosed information,[134] but do not set out an obligation to refrain from reviewing the document or using the inadvertently disclosed information. Some of these jurisdictions have modified Model Rule 4.4(b) to impose obligations to stop reading the document or to return the document.[135] The second group adopt the predecessor to Model Rule 4.4(b), ABA Opinion 92-368.[136] These jurisdictions require the receiving attorney to notify the sender, stop reviewing the document, and follow the sender's instructions on disposition of the document.[137] The third category are jurisdictions that have not specifically addressed the issue of inadvertent disclosure of information.[138] In these jurisdictions, the receiving attorney is left to make a judgment call concerning his response to receiving the information. Finally, some jurisdictions have taken completely different approaches.[139] For example, Massachusetts has said that the receiving attorney must reject the sender's request to return the document in order to zealously represent the receiving attorney's client.[140]

A jurisdiction's position on inadvertent disclosure of information and the receiving attorney's duties will provide guidance to an attorney who accidentally discovers metadata that is confidential or work product. However, these opinions do not provide much guidance to an attorney considering engaging in active mining for metadata. Those attorneys are left to determine whether their jurisdiction is likely to consider such actions dishonest and deceitful and therefore in violation of Model Rule 8.4(c)[141] or its equivalent.

V. Proposal for Army Action

The daily use of word processing software and frequent electronic mailing of documents in the Army requires the Army JAG Corps to address the issues associated with metadata. The scope of the metadata problem is difficult to determine because individuals may privately obtain and use confidential information without the knowledge of the party sending the document. However, the importance of the concepts of confidentiality, attorney work product, the deliberative process privilege; the threat posed by metadata; and the disagreements among the jurisdictions that have addressed the issue, show that a response from the Army JAG Corps is necessary. This response should include an opinion specifically addressing metadata under AR 27-26, a follow-on revision of AR 27-26, the procurement of commercial metadata scrubbing software, and training for all legal personnel on metadata.

A. Issue an Opinion on Metadata in the Army

The first step in addressing the issue of metadata in the Army JAG Corps should be the issuance of an opinion addressing metadata under AR 27-26. The Army Rules "govern the conduct of the lawyer in the performance of the lawyer's official responsibilities."[142] Lawyers subject to the Army Rules are "also subject to the rules promulgated by their licensing authority or authorities."[143] The metadata rule proposed in this article is equally or more restrictive than any state licensing authority that has addressed the topic. Therefore, an Army lawyer following the Army Rules would not be in danger of violating state ethics rules.

1. Require Senders to Scrub Documents

The Army opinion should go further than just requiring attorneys to take "reasonable steps" to protect client confidences and require attorneys to scrub documents for metadata. Army lawyers should scrub documents prior to sending them

---

[134] MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2008).

[135] *See*, *e.g.*, ARIZ. RULES OF PROF'L CONDUCT R. 4.4(b) (2004); LA. RULES OF PROF'L CONDUCT R. 4.4(b) (2006); N. J. RULES OF PROF'L CONDUCT R. 4.4(b) (2008).

[136] Perlman, *supra* note 133, at 783.

[137] ABA Standing Comm. on Ethics and Prof'l Responsibility, Formal Op. 92-368 (1992).

[138] Perlman, *supra* note 133, at 783.

[139] *Id.*

[140] Mass. Bar Ass'n, Op. 99-4 (1999).

[141] MODEL RULES OF PROF'L CONDUCT R. 8.4(c) (2008).

[142] *Id.* R 8.5(f)(1).

[143] *Id.* R. 8.5(f).

electronically outside the organization or to anyone not representing the same client as the sending attorney.[144] The opinion should also require Army lawyers to scrub documents posted to any internet site, including an office website or JAGCNet. The ABA and the jurisdictions reaching a similar conclusion have based their opinions on the obligation of attorneys to take reasonable steps to protect confidential information.[145] The comments to Model Rule 1.6 explicitly includes this obligation by stating "[w]hen transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients."[146] While the comments to Army Rule 1.6 do not contain identical language, the requirement to take reasonable steps to protect client information is implied. The comments in AR 27-26 discuss measures Army lawyers should take to protect client confidences, including having private offices and controlling access to automated data processing systems or equipment.[147] This discussion of measures that should be taken to ensure confidentiality implies an obligation to take reasonable steps to protect client confidences.

The ABA and the jurisdictions that have addressed metadata have not imposed an affirmative obligation to scrub documents for metadata. However, they uniformly require the sending attorney to take reasonable precautions to prevent the disclosure of confidential information through metadata.[148] Rather than restating this obligation and setting out factors to determine whether the attorney took reasonable steps, the Army should impose a rule that requires scrubbing documents. Such a rule would reiterate the important role that confidentiality plays in the legal profession, especially in the realm of Legal Assistance and Trial Defense Service. With advances in technology and commercially available software, such a rule is not unreasonable and could be implemented at a reasonable cost to the Government.

Army lawyers have several methods available to scrub documents prior to sending them. One option is to manually disable metadata through the word processing software, which Microsoft Word allows users to do.[149] Another option available to scrub a document is to print the document and then send it through a digital sender. A digital sender creates an image of the document that is opened with Adobe Acrobat. Digital senders are available to most Army lawyers, even in a deployed environment. Finally, Army lawyers can use commercial software that scrubs documents when they are attached to e-mail messages.

An Army opinion requiring that documents be scrubbed of metadata is preferable for several reasons. This requirement eliminates the need to analyze the factors set out in the ABA and state opinions. The requirement allows Army lawyers to know they have acted reasonably. In the event confidential metadata were still sent, a jurisdictional licensing authority would be unlikely to substantiate an ethical violation because the attorney took reasonable steps to prevent the disclosure. Finally, such an opinion provides the ultimate protection for the important concept of confidentiality by ensuring that all Army lawyers are using the best measures available to prevent disclosure of confidential information in metadata.

2. Prohibit the Mining of Metadata

The Army opinion should clearly prohibit mining for metadata as well as reviewing or using inadvertently discovered metadata. This course of action is the only result that gives the concepts of confidentiality, attorney work product, and the deliberative process privilege the protection they deserve. In addition, this approach promotes a legal profession that encourages integrity and advances the public image of attorneys. Allowing or sanctioning mining for metadata reinforces the public image of attorneys as dishonest and determined to do whatever it takes to see that their side wins rather than working to achieve justice.

However, AR 27-26, as currently stated, presents some issues with an Army opinion that prohibits mining for metadata. The best approach would be to treat mining for metadata as dishonest and deceitful, as New York,[150] Alabama,[151] and

[144] For example, a trial counsel sending a proposed stipulation of fact to his chief of military justice would not be required to scrub the document, but would be required to scrub it before sending it to defense counsel.

[145] *See* MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 17 (2008); ARIZ. RULES OF PROF'L CONDUCT R. 1.6 cmt. 19 &20 (2004); N.C. RULES OF PROF'L CONDUCT R. 1.6 cmt. 17 &18 (2008).

[146] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 17.

[147] AR 27-26, *supra* note 3, R. 1.6 cmt.

[148] *See* discussion *infra* Part III.

[149] *See* Lieutenant Colonel Charlotte R. Herring, Judge Advocate's IT Survival Guide, Tip #10—Hidden metadata and what to do with it! (n.d.) (attached at Appendix B).

[150] N.Y. Comm. on Prof'l Ethics, Op. 749 (2001).

Maine[152] do. If mining for metadata is considered dishonest and deceitful, it would violate Army Rule 8.4(c).[153] This rationale makes sense because mining for metadata is similar to an attorney going through another attorney's briefcase while the first attorney is briefly called away from a meeting.[154] You cannot conclude anything but that this conduct is dishonest and deceitful.

The more difficult problem for the Army Rules is their application to the issue of accidental discovery of metadata. As discussed below, AR 27-26 should be revised to include a Rule 4.4(b). Until this is done, the rules still provide a basis for imposing an obligation on a receiving attorney to refrain from reviewing or using inadvertently discovered metadata. Because of the importance of the concepts of confidentiality, attorney work product, and the deliberative process privilege, reviewing and using inadvertently discovered metadata could be determined to be prejudicial to the administration of justice and therefore violate Army Rule 8.4(d).[155] Alternatively, the Army could adopt the rationale of ABA Opinion 92-368,[156] since that opinion interpreted the same rules that are found in AR 27-26.[157] An opinion that prohibits mining for metadata, as well as prohibiting the reviewing or using of inadvertently discovered metadata, would best serve the Army legal community.

B. Revise Army Regulation 27-26

The second step the Army JAG Corps should take to effectively address the handling of metadata is to revise AR 27-26. The legal profession has changed a great deal since 1992, when AR 27-26 was last updated.[158] One of the primary changes has been the increased use of technology. Although no Army regulation could be updated frequently enough to keep pace with technology, it is time for AR 27-26 to be revised. Chief among the issues that should be addressed are two that the issue of metadata raises. First is the absence of any explicit requirement in Rule 1.6 or its comments for an attorney to exercise reasonable care to protect confidential information, as discussed earlier.

The second issue that metadata raises is the lack of a Rule 4.4(b) that deals with receipt of inadvertently sent information. Not only does this rule need to be added, but the rule should also be broader in scope than Model Rule 4.4(b).[159] Model Rule 4.4(b) only requires an attorney receiving an inadvertently sent document to notify the sender.[160] To truly protect confidentiality and illustrate its importance in the legal profession, Rule 4.4(b) should prohibit the receiving attorney from further reviewing the document or from any use of the material that was inadvertently disclosed.[161] This modification would not only better address the handling of metadata, but also provide improved protection for confidential information in whatever format it may be sent.

C. Procure Commercial Software

As a third step, the Army JAG Corps should procure commercial metadata scrubbing software. This software would facilitate the requirement to scrub documents for metadata. Although Microsoft Word users have the ability to disable metadata, the process must be done for each document. Mandating document scrubbing and training in this procedure may make the practice second nature, but a better way to ensure documents are scrubbed is through the use of commercial metadata scrubbing software. Several versions of this software are available that prevent a user from sending an unscrubbed document.[162] The software should be set up to prompt the sender to scrub any document attached to an e-mail. If the e-mail

---

[151] Ala. State Bar Office of the Gen. Counsel, Op. 2007-02 (2007).

[152] Me. Prof'l. Ethics Comm., Op. 196 (2008).

[153] AR 27-26, *supra* note 3, R. 8.4(c).

[154] *See* ABA Standing Comm. on Ethics and Prof'l Responsibility, Formal Op. 92-368 (1992).

[155] AR 27-26, *supra* note 3, R. 8.4(d).

[156] ABA Standing Comm. on Ethics and Prof'l Responsibility, Formal Op. 92-368 (1992).

[157] AR 27-26, *supra* note 3.

[158] *Id.*

[159] MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2008).

[160] *Id.*

[161] *See, e.g.*, ME. RULES OF PROF'L CONDUCT R 4.4(b) (effective Aug. 1, 2009).

[162] Commercial software being considered by the Army JAG Corps includes Esquire Innovations, Payne's Metadata Assistant, and iScrub. Telephone Interview with Erin Chisman, Info. Tech. Division, Office of The Judge Advocate General, U.S. Army, in Charlottesville, Va. (18 Dec. 08).

is being sent internally to someone representing the same client, the sender can choose not to scrub the document. Large law firms have recognized the problem of metadata and use this type of software to address the problem.[163] The Army JAG Corps, one of the largest law firms in the nation, should follow suit.

D. Institute a Training Requirement

Finally, the Army JAG Corps should require mandatory training. Many judge advocates may be unaware of metadata and the dangers it poses.[164] To address this lack of understanding, the Army JAG Corps should institute a requirement that all personnel—judge advocates, Department of the Army civilian attorneys, and paralegals—be trained on the issues associated with metadata. The Judge Advocate General's Legal Center and School could provide this training during the Basic and Graduate Courses, the Basic and Advanced Non-Commissioned Officer Courses, as well as the short courses. The training could also be accomplished during the Trial Counsel and Defense Counsel Assistance Program seminars. Finally, internal office professional development programs could cover the issue. Whatever the method, Army JAG Corps personnel need to be more aware of the implications of metadata, be trained on how to properly handle it, and be aware of their licensing jurisdiction's rules.[165]

VI. Conclusion

Recall the scenario, discussed earlier,[166] where two opposing lawyers are in a meeting and one attorney is briefly called away. While he is gone, the other attorney rifles through his briefcase looking for confidential information or attorney work product that could give him an advantage in the case.[167] All jurisdictions would agree that this behavior violated their ethical rules, yet this is akin to what happens when an attorney receives a document electronically and mines the document for metadata. Several jurisdictions have failed to give the concepts of confidentiality, attorney work product, and the deliberative process privilege the protection they deserve by improperly concluding that this conduct does not violate ethical rules. The Army needs to address this problem by taking a firm stand to protect confidentiality, attorney work product, and the deliberative process privilege, as well as to uphold the integrity of our profession. In the meantime, judge advocates must be attentive to the dangers of metadata and should take precautions to avoid the inadvertent transfer of sensitive information. Judge advocates should, at a minimum, familiarize themselves with the concept of metadata and should take prudent steps, including the scrubbing of documents, to protect client confidences and internal deliberations from undue disclosure.

---

[163] E-mail from Jeff Chapuran, Partner, Stoll, Kennon & Ogden, Attorneys at Law, Lexington, Ky., to the author (Oct. 8, 2008, 11:14 EST) (on file with author); e-mail from Steve Barham, Partner, Chambliss, Bahner & Stoephl, Attorneys at Law, Chattanooga, Tenn., to the author (Dec. 19, 2008, 11:31 EST) (on file with author).

[164] Prior to writing this article, the author did not appreciate the full scope of the problem. Although familiar with the ability to right-click on a file name and view the file's properties, the author did not have a full grasp of what could be uncovered by mining for metadata. Nor did the author understand the measures that could be taken to scrub documents. The author was not alone in this level of understanding, as many other judge advocates he talked to responded with blank stares when he told them the topic of this article. This ignorance does not appear to be unique to the Army JAG Corps. In a 2006 article, Sharon Nelson and John Simek indicated that when they lecture attorneys on the topic, "about half of the average audience has no idea what metadata is." Sharon D. Nelson & John W. Simek, *Metadata: What You Can't See CAN Hurt You*, LAW PRACTICE (ABA Law Practice Mgmt. Section, Chicago, Ill.), Mar. 2006, at 28.

[165] Several jurisdictions address training in their opinions on metadata. *See, e.g.*, N.Y. Comm. on Prof'l Ethics, Op. 782 (2004) (indicating that attorneys must "stay abreast of technological advances"); Ethics Comm. of the Colo. Bar Assoc., Ethics Op. 119 (2008) (stating that attorneys "may not limit the duty [to exercise reasonable care in avoiding sending metadata] by remaining ignorant of technology relating to metadata."); Me. Prof'l Ethics Comm., Op. 196 (2008) (stating it is not reasonable "for an attorney today to be ignorant of the standard features and capabilities of word processing and other software used by that attorney, including their reasonably known capacity for transmitting certain types of data that may be confidential").

[166] *See* discussion *supra* Part V.A.2.

[167] *See* ABA Standing Comm. on Ethics and Prof'l Responsibility, Formal Op. 92-368 (1992).

Appendix A

State Bar Ethics Opinions on Metadata

Note—this information is current as of 23 February 2009 and was obtained by conducting searches on both Lexis and Westlaw for "metadata" in each state's ethics opinions.

State	Opinion #	Date	Summary
Alabama	2007-02	3/14/07	Sender—obligation to take reasonable steps to avoid disclosure of metadata; what is reasonable will depend on circumstances. Receiver—mining is a violation of rules, except in electronic discovery as directed by a court.
Alaska	None found		
Arizona	07-03	11/07	Sender—must take reasonable steps to prevent disclosure; what is reasonable will depend on circumstances; specifically states that you should not use templates. Receiver—may not take measures to intentionally find metadata. If some metadata is found inadvertently and knows/should know it is confidential, they must leave it alone and notify sender.
Arkansas	None found		
California	2007-174		Opinion address releasing electronic copies of records to former clients but does say when doing so an attorney has a duty to take reasonable measures to ensure no metadata containing information from another client is on the files.
Colorado	119	5/17/08	Sender—has a duty to exercise reasonable care to guard against disclosure. Receiver—can search and review but if finds metadata and knows or should know it was inadvertent, must promptly notify sender.
Connecticut	None found		
Delaware	None found		
District of Columbia	341	9/07	Sender—must take reasonable steps to avoid sending. Mining—prohibited only when attorney has actual knowledge that metadata was inadvertently sent.
Florida	06-2	9/15/06	Sender—must take reasonable steps to prevent disclosure. Receiver—prohibits mining because it is dishonest and deceitful.
Georgia	None found		
Hawaii	None found		
Idaho	None found		
Illinois	None found		
Indiana	None found		
Iowa	None found		
Kansas	None found		
Kentucky	None found		
Louisiana	None found		
Maine	Opinion 196	10/21/08	Sender—must take reasonable steps to avoid transmitting metadata. Receiver—prohibits mining as dishonest and prejudicial to the administration of justice.
Maryland	2007-09		Sender—must take reasonable measures to prevent disclosure. Receiver—no prohibition on mining based on Maryland not having added 4.4(b) to its rules.
Massachusetts.	None found		
Michigan	None found		
Minnesota	None found		
Mississippi	None found		
Missouri	None found		
Montana	None found		

Nebraska	None found		
Nevada	None found		
New Hampshire	None found		
New Jersey	None found		
New Mexico	None found		
New York	Opinion 782 and 749	12/8/04 and 12/14/01	Sender—must exercise reasonable care to prevent disclosure. Receiver—cannot use technology to discover metadata.
North Carolina	2009 Proposed Formal Opinion 1	1/22/2009	A proposed formal opinion was released in Jan 2009. The proposed opinion requires senders to exercise reasonable care and prohibits the mining of metadata.
North Dakota	None found		
Ohio	None found		
Oklahoma	None found		
Oregon	None found		
Pennsylvania	2007-500	2007	No explicit rule on mining—up to each individual attorney based on their judgment and the facts. Factors to consider include: nature of the info received, how and from whom received, attorney-client privilege and work product rules, common sense, reciprocity, and professional courtesy.
Rhode Island	None found		
South Carolina	None found		
South Dakota	None found		
Tennesse	None found		
Texas	None found		
Utah	None found		
Vermont	None found		
Virginia	None found		
Wash.	None found		
West Virginia	None found		
Wisconsin	None found		
Wyoming	None found		

Appendix B

Tip #10 - Hidden metadata and what to do with it!

Metadata is information on who created the file, when it was created/modified/accessed, what drive information was stored on, and even printed. Obviously, in our profession, this information may be confidential, or even privileged. Is there any way to stop this information from being forwarded with your Word/Powerpoint/and Excel documents? YES! In fact, it's not just text and office files. Even DVD's and camera's add their serial number in their files. This information can then be cross referenced with warranty cards to find owners or scanned on MySpace or Flickr by using the EXIF (image file format used by digital cameras) metadata on the files.

First of all, go to "My Documents." Open any document of your choice. Click on "File" menu, and chose "Properties." This is the information that I am talking about - this is metadata. More likely than not, you are looking at your name, or if it is a document someone else created, their name. But wait a minute -- it's nobody's name you recognize! Oh, then the person who sent it to you did not create it. You can look and see when it was created, if it was modified, and when. Obviously, this information may be important in many instances.

Do we as an Army agency want to forward that information on to a recipient? No. For security purposes, less is more. Therefore, what is the first step toward not forwarding metadata? Change your settings in Word! And once you change them in Word, it applies to other Office programs, as well.

If you are using Word 2003, open a new document. Click on "Tools," then "Options," and last, "Security." Under "Privacy Options," click on "Remove personal information from file properties on save," "Warn before printing, saving, or sending a file that contains tracked changes or comments," and "Store random number to improve merge accuracy." Regretfully, however, you have to do this for EVERY document you generate as the "Remove personal information from file properties on save" cannot be done to the Word template from your computer.

Also, the settings differences between Word 2003 & 2007 is substantial. To get to those same settings in Word 2007, click on the "Office" button (upper right hand corner of the screen) then the "Word Options" button. Choose "Trust Center" and then click on the "Trust Center Settings" button (lower right). Once in the settings box, select “Privacy Options” then under the "Document Specific Settings" the settings discussed above will be in that group. You will need to do this for every document you generate, just like in Word 2003.

This is just one step in the effort to protect JAGC metadata. Stand by as ITD investigates more ways to protect our information when we create it!

Charlotte R. Herring
LTC, JA
Chief, Information Technology Division