Journal of Technology
Law & Policy

Volume XVI – Fall 2015

ISSN 2164-800X (online)

DOI 10.5195/tlp.2015.176

http://tlp.law.pitt.edu

The Use of Non-Confidential and Limited Confidential Information Obtained by Metadata Mining Outside the Context of Discovery Should Be Ethically Permissible

Michelle K. Chu

The Use of Non-Confidential and Limited Confidential Information Obtained by Metadata Mining Outside the Context of Discovery Should Be Ethically Permissible

Michelle K. Chu[*]

INTRODUCTION

Imagine that a lawyer representing the buyer in the purchase of a company receives an electronic word document for the sale agreement from opposing counsel. The receiving lawyer[1] clicks on the "View Markup" button, allowing him to see the "Track Changes"[2] that the sending lawyer[3] made while drafting the document. One of the "Track Changes" is a calculation for the lowest price the seller is willing to accept, a note the sending lawyer did not intend for the receiving lawyer to see.

Now, imagine in the above situation that the negotiations are supposed to be exclusive. Suspicious that the seller is not exclusively negotiating with the buyer, the buyer's lawyer confirms his suspicion after examining the authorship of the document and discovers that its author is another potential buyer.

Consider the two above situations. What was the sending lawyer's duty of care in sending the document? Was it ethically permissible for the receiving lawyer to "mine" or look for this embedded information, known as metadata, and use it for his client's benefit? Does the receiving lawyer need to notify the sending lawyer of the transmission of metadata?

Technological advancements in the past few decades have increased electronic communications within the practice of law. Electronic communications have allowed lawyers to more easily communicate with their clients and opposing counsel, engage in electronic discovery, conduct legal research more efficiently, and file documents

[*] J.D. Benjamin N. Cardozo School of Law, 2015; B.S. Carnegie Mellon University, 2012. Thanks to Professor Lester Brickman and JS for their feedback.

[1] Throughout this paper, "receiving lawyer" will be used to represent a lawyer who receives a document.

[2] "Track Changes" is a tool in certain word processing programs that allows multiple users to make changes to a document while keeping track of those changes. If a tracked change is not properly removed, another user may be able to view a change not intended for him to view.

[3] Throughout this paper, "sending lawyer" will be used to represent a lawyer who sends a document.

Volume XVI – Fall 2015 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2015.176 ● http://tlp.law.pitt.edu

electronically.[4] However, the ease and efficiency of electronic communications, combined with the large volume of electronically stored files being exchanged, often leads to the inadvertent transmission of information contained in metadata by the sending lawyer. Consequently, the receiving lawyer may be able to extract the information or "mine" for metadata, like in the problems above.

Part I of this paper provides background on the significance of metadata and metadata mining, in addition to techniques a sending lawyer can limit transmission of metadata. Although metadata may be exchanged between lawyers and non-lawyers alike, this note focuses on the exchange of metadata between lawyers. Part II discusses the duties of sending and receiving lawyers regarding metadata mining. This note primarily addresses metadata mining outside the context of discovery where opposing counsel voluntarily exchange electronic documents. Part III addresses the different approaches the American Bar Association ("ABA") and state bar associations have taken regarding metadata mining. Part IV proposes that the use of non-confidential information obtained by metadata mining should be ethically permissible outside the context of discovery. Additionally, the use of confidential information obtained by mining outside the context of discovery should be treated similar to inadvertent disclosures of confidential information within the context of discovery, and be ethically permissible when the sending lawyer's duty of reasonable care rises to the level of negligence.

I. METADATA & METADATA MINING

A. Significance of Metadata and Metadata Mining

Metadata is "data about data;" it is information about electronically stored files that is hidden or embedded within those files or in a linked database.[5] The two main categories of metadata are system metadata and application metadata.[6] System metadata is information on a computer's hard drive or memory, but not embedded within a document.[7] Examples of system metadata include, but are not limited to, the size and location of each file on a computer.[8] Application metadata is information

[4] Elizabeth W. King, *The Ethics of Mining for Metadata Outside Formal Discovery*, 113 PENN ST. L. REV. 801, 810 (2009).

[5] Judge Herbert B. Dixon, Jr., *I Never Meta Data I Didn't Like*, 48 NO. 2 JUDGES' J. 37, 37 (2009).

[6] *Id.*

[7] *Id.*

[8] *Id.*

embedded in a file that is not immediately visible to the viewer.[9] Examples of application metadata include, but are not limited to, file designation, create and edit dates, authorship, comments, and edit history.[10] This note will focus on application metadata because it is the category of metadata that is more commonly exchanged between lawyers. Metadata found in email, documents created by word processing programs, and spreadsheets are the types of metadata that lawyers are most concerned about[11] because those documents are most frequently exchanged between lawyers.

Metadata mining is the extraction of embedded information of an electronic document, which may or may not be confidential, and may be done with or without the sending lawyer's permission.[12] It may be used in both litigation and transactional contexts.[13] Metadata mining has many useful applications including authenticating documents and determining whether documents are genuine. For example, parties can easily meet authentication requirements under the Federal Rules of Evidence ("FRE") and applicable state law when they are able to establish information such as the date the document was created and the identity of the party who created it.[14] Metadata can also be used to determine whether documents are genuine by showing whether a document has been intentionally or inadvertently modified.[15] There are also certain types of cases, such as cases claiming discrimination, that often do not yield much evidence with material evidentiary value.[16] Information obtained by metadata mining is one way to strengthen such cases.

Mining for information important to the sending or opposing lawyer is one of the most important applications of metadata mining.[17] Although a sending lawyer may edit or delete text, the edited or deleted text may still be embedded in the

[9] *Id.*

[10] SHIRA A. SCHEINDLIN & DANIEL J. CAPRA, ELECTRONIC DISCOVERY AND DIGITAL EVIDENCE IN A NUTSHELL 158 (2009).

[11] Philip J. Favro, *A New Frontier in Electronic Discovery: Preserving and Obtaining Metadata*, 13 B.U. J. SCI. & TECH. L. 1, 7 (2007).

[12] Andrew M. Perlman, *The Legal Ethics of Metadata Mining*, 43 AKRON L. REV. 785, 786 (2010). Throughout this paper "metadata mining" refers to mining for metadata without permission.

[13] *Id.* at 787.

[14] Favro, *supra* note 11, at 11.

[15] *Id.*

[16] *See generally* Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640 (D. Kan. 2005).

[17] Tomas J. Garcia & Shane T. Tela, *Jurisdictional Discord in Applying Ethics Guidelines to Inadvertently Transmitted Metadata*, 23 GEO. J. LEGAL ETHICS 585 (2010).

electronic code of the document.[18] Failing to remove this metadata may reveal important information in the contents of previous edits such as negotiation strategies, new interests, abandoned strategies, and demands.[19]

B. Ways to Limit Metadata Transmission

There are many ways for a sending lawyer to limit the transmission of metadata, which vary in cost, efficacy, and technical difficulty. None of these methods will remove all metadata from a document, but they certainly limit their transmission.[20] Many word processing programs have free metadata removal options, such as PDF[21] conversion, searching for and removing hidden text, and manually removing comments from a document.[22] These metadata removal options are free and user friendly, but will not remove all of the metadata.[23] In fact, although PDF conversion is a proposed way of limiting metadata transmission, it is often not practical, particularly in a transactional context in which lawyers exchange documents back and forth to each other to edit.

On the other hand, metadata scrubbers are significantly more effective than the aforementioned methods. Metadata scrubbers are relatively inexpensive software that remind the user of the presence of metadata and then "scrub" or remove the most important parts of metadata if the user wishes, while maintaining the content in the original document.[24] In addition to metadata scrubbers, some firms may even consider expanding their information technology departments or hiring electronic discovery consultants for certain cases.[25] A sending lawyer's tactics to limit the transmission of metadata should correlate with the complexity of a firm's practice and its volume of electronically stored files.

[18] *Id.* at 588.

[19] *Id.*

[20] Adam K. Israel, *To Scrub or Not to Scrub: The Ethical Implications of Metadata and Electronic Data*, 60 ALA. L. REV. 469, 475 (2009).

[21] PDF stands for Portable Document Format. PDF is a file format that provides an electronic image of text that looks like a printed document. It can be viewed, printed, and electronically transmitted. (*PDF Definition*, GOOGLE, https://www.google.com/search?q=pdf+definition&ie=utf-8&oe=utf-8 (last visited Apr. 20, 2015)).

[22] Israel, *supra* note 20, at 475.

[23] *Id.*

[24] *Id.*

[25] *Id.*

II. Duties Related to Metadata Mining for Sending and Receiving Lawyers

A. Rules Governing Metadata Mining Within the Context of Discovery

The rationale behind permitting metadata mining *within* the context of discovery may help answer the question of whether it is ethically permissible for a receiving lawyer to mine for metadata *outside* the context of discovery. The 2006 revisions to the Federal Rules of Civil Procedure ("FRCP") considered technological change by acknowledging metadata, even though metadata was not explicitly mentioned. FRCP 34(a) created a new category of discoverable material, electronically stored information ("ESI"),[26] which means that electronic information, such as metadata, may be ascertained during discovery.[27] Additionally, FRCP 34(b) allows the receiving lawyer to specify the format in which the ESI is to be produced.[28] For example, a document may need to be produced in its original format, meaning all metadata is intact.[29] On the other hand, if metadata likely contains confidential information, the parties may agree to have the document scrubbed.[30]

Because a receiving lawyer is entitled to documents with metadata intact under the new rules, a sending lawyer has a duty to take reasonable measures to ensure that metadata is kept intact.[31] However, a sending lawyer may object to a requested form of production.[32] For example, the sending lawyer may already know that there will likely be confidential information in a document requested in its original format. If the sending and receiving lawyers cannot agree on a format, the court will decide for them.[33] Although the revised FRCP do not specifically address metadata mining, there is a presumption that metadata mining is permissible within the context of discovery because of the potential relevance of the metadata and because ESI, including metadata, is discoverable.[34]

[26] FED. R. CIV. P. 34(a).

[27] FED. R. CIV. P. 34(a)(1)(A).

[28] FED. R. CIV. P. 34(b)(1)(C).

[29] *Id.*

[30] *Id.*

[31] FED. R. CIV. P. 26(f), 16(b).

[32] FED. R. CIV. P. 34(b) advisory committee's note.

[33] *Id.*

[34] King, *supra* note 4, at 811.

In addition to the FRCP, the FRE provide states with guidance on how to treat inadvertent disclosures of confidential information in documents exchanged during discovery. The FRE may also help determine whether it is ethically permissible for a receiving lawyer to mine for metadata outside the context of discovery. Although the FRE do not explicitly mention metadata, under FRE 502(b), an inadvertent disclosure will not be considered a waiver if the sending lawyer took "reasonable steps" to prevent the disclosure and promptly rectified the error once he discovered the mistake.[35] Relevant factors in determining "reasonable steps" include the number of inadvertent disclosures compared to the volume of information subject to review, the time constraints for production, use of analytical software and effective search terms, implementation of an efficient system of records management before litigation arises, and the number of levels of review and personnel used to review the data.[36] FRE 502(a) affords further protection by providing that even if a party inadvertently produces confidential information during discovery and waiver is found, the waiver only applies to the actual material disclosed.[37] The sending lawyer would not be required to produce related confidential information.

Although there are no bright-line rules and what is "reasonable" is considered on a case-by-case approach, FRE 502 is basically a negligence test.[38] Ultimately, there is a tendency towards non-waiver[39] because the mistakes made would have to rise to the level of negligence, mistakes no reasonable lawyer would make.

B. Ethics Rules Implicated in Metadata Mining Outside the Context of Discovery

While the FRCP is clear about metadata mining within the context of discovery, they do not provide guidance to lawyers who voluntarily exchange documents outside the context of discovery. Additionally, although the FRE discusses inadvertent disclosures of confidential information within the context of discovery, no commentator has thus far discussed the ethical implications of the FRE on metadata mining either within or outside the context of discovery. Document exchanges occur in other contexts, such as the transactional context and the time

[35] FED. R. EVID. 502(b).

[36] FED. R. EVID. 502(b) advisory committee's note.

[37] FED. R. EVID. 502(a).

[38] SCHEINDLIN & CAPRA, *supra* note 10, at 276.

[39] Louise L. Hill, *Emerging Technology and Client Confidentiality: How Changing Technology Brings Ethical Dilemmas*, 16 B.U. J. SCI. & TECH. L. 1, 52 (2010).

periods before and after discovery.[40] To date, there have been no judicial cases involving metadata mining outside the context of discovery.

However, metadata mining implicates several of the ABA Rules of Professional Conduct ("Model Rules").[41] Although all states have their own ethical rules of professional conduct, they all use the Model Rules as a guide for writing their rules.[42] Additionally, although the Model Rules do not explicitly mention metadata, they still provide guidance for the boundaries where metadata mining falls within legal ethics.[43]

1. Model Rules 1.1 Competence, 1.3 Diligence

Under Model Rule 1.1, lawyers have a duty to provide to their clients competent representation, which "requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation."[44] Under Model Rule 1.3, they must also act with reasonable diligence in representing a client.[45] In order to achieve these requirements, lawyers should stay abreast of technological changes, particularly those that impact their practice of law.[46] By no means does this indicate that lawyers need to become experts in technology, but they must understand the risks associated with the metadata in their ESI, learn methods of limiting the transmission of metadata, and ensure that their colleagues and subordinates understand metadata as well.[47]

2. Model Rule 1.6(a) Confidentiality

Under Model Rule 1.6, lawyers must not reveal information relating to the representation of a client.[48] Confidentiality is at the core of the attorney-client relationship. Because electronic communication is virtually necessary in today's practice of law, lawyers must be careful not to reveal confidential information in both the face of a document and its metadata. These disclosures include not only the confidential information itself, but also information that could reasonably lead to the

[40] *Id.* at 59.

[41] Crystal Thorpe, *Metadata: The Dangers of Metadata Compel Issuing Ethical Duties to "Scrub" and Prohibit the "Mining" of Metadata*, 84 N.D. L. REV. 257, 269 (2008).

[42] *Id.* at 270.

[43] *Id.* at 270.

[44] MODEL RULES OF PROF'L CONDUCT R. 1.1 (2012).

[45] MODEL RULES OF PROF'L CONDUCT R. 1.3 (2012).

[46] MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. 8 (2012).

[47] Thorpe, *supra* note 41, at 270; King, *supra* note 4, at 829.

[48] MODEL RULES OF PROF'L CONDUCT R. 1.6 (2012).

discovery of the confidential information by a third party.[49] Therefore, Rule 1.6 implicates a duty to remove metadata (unless a court orders the disclosure of documents with their metadata intact) from documents related to client representation in order to maintain confidentiality.[50]

3. *Model Rule 4.4 Respect for Rights of Third Persons*

Under Model Rule 4.4(b), a lawyer who receives a document or ESI relating to the representation of a sending lawyer's client and knows or reasonably should know that the document or ESI was inadvertently sent must promptly notify the sending lawyer.[51] Rule 4.4(b) does not discuss metadata mining, but only imposes an obligation of notice on the receiving lawyer in the event of an inadvertent disclosure in order to give the sending lawyer the opportunity to take protective measures.[52] It does not require the receiving lawyer to do anything else, such as return the document.[53]

4. *Model Rule 8.4 Misconduct*

Under Model Rule 8.4, lawyers engage in professional misconduct when their actions involve "dishonesty, fraud, deceit, or misrepresentation."[54] Some believe that metadata mining falls under this definition of professional misconduct because it constitutes dishonesty or deceit.[55] When sending lawyers send a document, they intend that receiving lawyers only view the information on the face of the document.[56] While lawyers should do everything they can within the bounds of the law to represent their clients' best interests, a receiving lawyer's metadata mining may violate a sending lawyer's work product privilege.[57] Metadata mining entails receiving lawyers to look beyond the face of a document in search for information that sending lawyers inadvertently leave, in an attempt to gain an advantage for their clients.

[49] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 4 (2012).

[50] Thorpe, *supra* note 41, at 272.

[51] MODEL RULES OF PROF'L CONDUCT R. 4.4 (2012).

[52] MODEL RULES OF PROF'L CONDUCT R. 4.4 cmt. 2 (2012).

[53] *Id.*

[54] MODEL RULES OF PROF'L CONDUCT R. 8.4 (2012).

[55] Thorpe, *supra* note 41, at 273.

[56] *Id.*

[57] *Id.*

III. Approaches to Metadata Mining

To date, the ABA, the Bar of the District of Columbia, and seventeen state bar associations have issued ethics opinions regarding metadata mining.[58] These opinions encompass the key questions posed at the beginning of this note: what is the sending lawyer's duty when transmitting electronic documents containing metadata; whether the receiving lawyer can mine the metadata, and whether the receiving lawyer must notify the sending lawyer if metadata is found. Excluding the ABA, all of the opinions establish that the sending lawyer has a duty of reasonable care to ensure that he does not reveal confidential information in the transmission of metadata.[59] Most of the opinions agree that the receiving lawyer has a duty to notify the sending lawyer of the transmission of metadata, some requiring actual knowledge of the inadvertent transmission to trigger the duty to notify.[60] However, there is much disagreement about whether the receiving lawyer is allowed to mine the metadata.[61] Ten of the opinions establish that metadata mining is always ethically impermissible; seven determined it is always ethically permissible; one states that metadata mining is ethically permissible in certain circumstances; and one leaves metadata mining to the discretion of the receiving lawyer.[62] Some opinions discuss metadata mining outside the context of discovery; others are not specific.[63]

A. Duties of Sending Lawyer: Largely One Approach

A sending lawyer always has the duty to maintain confidentiality relating to the representation of his client.[64] All of the state bar associations that have issued ethical opinions regarding metadata mining establish that in order to maintain confidentiality, the sending lawyer has a duty of reasonable care to ensure that he does not reveal confidential information in the transmission of metadata.[65] Although the ABA does not impose an explicit duty on sending lawyers like the state bar

[58] Am. Bar Ass'n, *Metadata Ethics Opinions Around the U.S.*, http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/metadatachart.html (last visited Mar. 3, 2015).

[59] *Id.*

[60] *See supra* note 58.

[61] *Id.*

[62] *Id.*

[63] *Id.*

[64] Model Rules of Prof'l Conduct R. 1.6 (2012).

[65] *Metadata Ethics Opinions Around the U.S.*, *supra* note 58.

associations do, it presumes that a sending lawyer's general duties regarding the confidentiality of client information under Rule 1.6 apply to metadata.[66]

B. Duties of Receiving Lawyer: Great Discrepancy in Approaches

1. "Ethically Impermissible" Approach

New York was the first state to address metadata mining (even before the ABA), concluding that metadata mining is unethical. New York imposes a duty to use reasonable care when communicating electronically on sending lawyers, which includes preventing the disclosure of metadata.[67] However, because confidentiality is vital for a strong lawyer-client relationship, metadata mining to obtain information that would otherwise be protected under confidentiality violates the public policy reasoning behind confidentiality.[68] Using this same reasoning, New York determined that a receiving lawyer must notify the sending lawyer that metadata was found, although the receiving lawyer may permissibly use the information mined.[69] Florida, Alabama, Maine, and Arizona have used similar reasoning to conclude that metadata mining is ethically impermissible.[70]

2. "Ethically Permissible" Approach

The ABA reads the addition of Rule 4.4(b) as requiring the receiving lawyer to notify the sending lawyer if metadata is found, but without an agreement explicitly prohibiting metadata mining, the receiving lawyer is free to mine.[71] The ABA imposes no additional duties on a sending lawyer in regard to metadata beyond the duty to maintain client confidentiality.[72] The ABA does, however, suggest methods for removing metadata from a file, including scrubbing the metadata, converting the file to a different format with less metadata, or negotiating a confidentiality agreement with the receiving lawyer to prohibit metadata mining.[73]

Following in the footsteps of the ABA's minority stance, Maryland also determined that metadata mining should be ethically permissible. Without an

[66] *Id.*

[67] N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 782 (2004).

[68] N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 749 (2001).

[69] Ass'n of the Bar of the City of N.Y. Comm. on Prof'l & Judicial Ethics, Formal Op. 2003–04 (2003).

[70] *Metadata Ethics Opinions Around the U.S.*, *supra* note 58.

[71] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 05-437 (2005).

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

[73] *Id.*

agreement with opposing counsel, the sending lawyer must take reasonable measures to avoid the disclosure of metadata. Maryland found that metadata mining is ethically permissible even more so than the ABA. Unlike the ABA, which determined that a receiving lawyer must promptly notify the sending lawyer upon discovery of inadvertent transmission of metadata, Maryland does not impose such a requirement.[74]

3. "Certain Circumstances" Approach

Washington D.C. allows metadata mining in certain circumstances.[75] Under this approach, a sending lawyer must take reasonable steps to maintain the confidentiality of his documents, which includes using reasonably available technological means to remove metadata from a document before sending it.[76] A receiving lawyer may ethically search and use metadata unless he has actual knowledge that the metadata was inadvertently sent.[77] A receiving lawyer has actual knowledge if the sending lawyer notifies him before he reviews the metadata that it was inadvertently sent or immediately notices upon review that the metadata was inadvertently sent.[78] However, if it is unclear that metadata contains confidential information, where the receiving lawyer does not have actual knowledge that the metadata was inadvertently sent, the receiving lawyer may continue to review the metadata.[79] Washington D.C. is the only jurisdiction to hold that in situations where confidentiality of metadata cannot be determined, the receiving lawyer's duty of representation trumps the duty of confidentiality, and the receiving lawyer can continue to review and use the metadata.[80]

4. "Professional Judgment" Approach

Pennsylvania is the only state bar association that has given discretion to the receiving lawyer to use his professional judgment in reviewing and using metadata.[81] However, the sending lawyer still has a duty of reasonable care in sending metadata and the receiving lawyer still has a duty to notify the sending lawyer of inadvertently sent metadata.[82]

[74] Md. State Bar Ass'n Comm. on Ethics, No. 2007–09 (2006).

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

[76] *Id.*

[77] *Id.*

[78] *Id.*

[79] *Id.*

[80] King, *supra* note 4, at 824.

[81] Pa. Bar Ass'n Comm. on Legal Ethics & Prof'l Responsibility, Formal Op. 2009–100 (2009).

[82] *Id.*

IV. Proposal: Using Non-Confidential Information and Certain Confidential Information Obtained by Metadata Mining Should Be Ethically Permissible

States that have yet to adopt ethical opinions about metadata mining should make metadata mining ethically permissible. Within the proposed regime of metadata mining of this note, sending lawyers should have a duty of reasonable care in sending electronic documents containing potentially confidential metadata. It should be ethically permissible for receiving lawyers to mine for metadata outside the context of discovery in order to fulfill their duties of competence and diligence when trying to find relevant information for a client's representation. Regarding the information obtained by metadata mining, receiving lawyers should be able to use all non-confidential metadata, whether or not its transmission was inadvertent. It should also be ethically permissible for receiving lawyers to use confidential metadata obtained by mining in limited situations and should be treated like inadvertent disclosure of confidential information within the context of discovery. This type of situation only arises when the sending lawyer did not act with reasonable care, violating both his ethical duties of confidentiality and competence. Additionally, upon discovering confidential metadata, the receiving lawyers should notify the sending lawyer immediately of its transmission in order for the sending lawyer to take protective measures.

A. Duties of Sending Lawyer: Duty of Reasonable Care

It is clear that sending lawyers have a duty of reasonable care in sending electronic documents with metadata,[83] but it is unclear what "reasonable" means.[84] State bar associations that have issued ethical opinions about metadata mining have considered certain factors in determining what "reasonable" care is.[85] Although they vary among state bar associations, factors include relevant considerations, such as the sensitivity of the information being transmitted; steps the sending lawyer took to prevent disclosure; the nature and scope of the revealed metadata; and the potential consequences of the inadvertent disclosure.[86] These factors are similar to the factors used in FRE 502.[87]

[83] *See supra* Section III.A.

[84] King, *supra* note 4, at 817.

[85] *Id.* at 817–18.

[86] *Id.*

[87] Fed. R. Evid. 502(b) explanatory note.

B. *Duties of Receiving Lawyer: Allowed to Mine for Metadata and Use Non-Confidential and Limited Confidential Metadata, but Duty to Notify*

Although it is clear that sending lawyers have a duty of reasonable care in sending electronic documents with metadata, there is great discrepancy in whether or not receiving lawyers are ethically permitted to mine for the metadata outside the context of discovery.[88] However, the opinions that prohibit metadata mining do not distinguish between non-confidential metadata and confidential metadata.[89] Receiving lawyers can mine for metadata in many different contexts, only some of which will reveal confidential information.[90]

It should be ethically permissible for receiving lawyers to be able to mine and use non-confidential metadata since there are no rules governing the use of non-confidential information. Furthermore, it should be ethically permissible for receiving lawyers to use confidential metadata obtained by mining in limited situations. Only if the sending lawyer did not act with reasonable care, violating both his ethical duties of confidentiality and competence, is it fair to the receiving lawyer to have confidentiality waived and be able to use the confidential information that he found by metadata mining. Inadvertent disclosures of confidential information obtained from metadata should be treated like inadvertent disclosures of confidential information within the context of discovery under FRE 502. Since confidentiality is required for the welfare of the client, it should only be when the sending lawyer's lack of reasonable care rises to level of negligence that the client loses confidentiality. The reasons listed below justify the proposed regime of metadata mining outside the context of discovery.

1. *The Duty of Confidentiality Still Trumps the Duty of Diligence*

Even if a lawyer inadvertently sends metadata, negligently or not, it is unlikely to be confidential because most electronic documents do not contain confidential metadata.[91] If a receiving lawyer subsequently mines for metadata, he is very likely to obtain non-confidential information that has very little material evidentiary value.[92] Even if a receiving lawyer obtains confidential metadata, a sending lawyer's lack of reasonable care would need to rise to the level of negligence before waiver of confidentiality could even be considered, similar to the test for waiver of confidentiality in inadvertent disclosures within the context of discovery. As with

[88] *Metadata Ethics Opinions Around the U.S.*, *supra* note 58.

[89] Perlman, *supra* note 12, at 792.

[90] *Id.*

[91] *Id.*

[92] *Id.*

Volume XVI – Fall 2015 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2015.176 ● http://tlp.law.pitt.edu

inadvertent disclosures analyzed under FRE 502, waiver of confidentiality is unlikely to happen. As a practical matter, once a receiving lawyer discovers confidential metadata, it is difficult to completely disregard it. However, the same problem exists in privilege review for the face of documents under FRE 502. Consequently, the duty of confidentiality still trumps the duty of competent representation.

2. Receiving Lawyers Who Mine for Metadata Provide Their Clients with Diligent and Competent Representation

There are legitimate reasons why a receiving lawyer would mine for metadata. For instance, metadata can be critical to establishing or supporting a claim or defense.[93] A lawyer would not be meeting his duties of competence and diligence if metadata mining would be helpful to his client's case and he did not pursue this strategy.[94] Because lawyers are becoming more knowledgeable about the risks associated with metadata and the ways to limit its transmission, it is now more reasonable to expect that sending lawyers will check documents for confidential metadata and limit its transmission before sending them.[95]

3. The Receiving Lawyer Notifies the Sending Lawyer of the Transmission of Metadata

A receiving lawyer who mines for metadata and knows or should know that it was inadvertently sent should promptly notify the sending lawyer. Under Model Rule 4.4(b), a lawyer who receives a document or ESI relating to the representation of a sending lawyer's client and knows or reasonably should know that the document or ESI was inadvertently sent must promptly notify the sending lawyer.[96] The same reasoning should apply to metadata mining because the receiving lawyer's notification allows the sending lawyer the opportunity to take protective measures.[97]

[93] *See generally* Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640 (D. Kan. 2005) (in this age discrimination case, the metadata in Microsoft Excel spreadsheets was critical for plaintiff Williams to demonstrate defendant's pattern of age discrimination by "reworking" pools of employees to pass an adverse impact analysis).

[94] *See supra* notes 44, 45.

[95] *Id.* at 793.

[96] MODEL RULES OF PROF'L CONDUCT R. 4.4 (2012).

[97] MODEL RULES OF PROF'L CONDUCT R. 4.4 cmt. 2 (2012).

4. *Metadata Mining Is Not Like Looking Through Someone's Briefcase*

Metadata mining does not fall within the definition of professional misconduct as "dishonesty, fraud, deceit, or misrepresentation."[98] Analogizing metadata mining to "searching an opponent's unattended briefcase during a deposition"[99] is incorrect.[100] This analogy is based on the mistaken idea that an electronic document contains only what is visible on its face and that sending lawyers only intend for receiving lawyers to view the visible portions of documents.[101] However, all a receiving lawyer does when he mines for metadata is look through the entirety of an electronic document. This should not fall under "dishonesty, fraud, deceit, or misrepresentation" because the inadvertent disclosure of metadata should be treated like inadvertent disclosures of an electronic document.[102]

5. *Sending Lawyers and Receiving Lawyers Equally Share the Burden*

Sending lawyers have a duty of reasonable care in reviewing and removing metadata from electronic documents before their submission[103] and have numerous ways of limiting their transmission of metadata.[104] One of the simplest and most effective ways for counsel to prevent metadata mining is to agree in advance with opposing counsel not to mine for metadata. However, both sides may not have the foresight to think metadata mining will be a problem. Additionally, because of the large volume of ESI involved in most litigation and transactional work, even the most diligent lawyer may inadvertently disclose confidential information.[105]

One of the arguments against making metadata mining ethically permissible is that metadata mining places the entire burden of ensuring that confidential information within metadata is not revealed in the transmission of an electronic document on the sending attorney.[106] Opponents of allowing metadata mining as ethically permissible also argue that metadata mining encourages sending lawyers to avoid creating metadata in the first place and deters them from sending documents

[98] MODEL RULES OF PROF'L CONDUCT R. 8.4 (2012).

[99] Miss. Bar Ethics Comm., Op. 259 (2012).

[100] Perlman, *supra* note 12, at 794.

[101] *Id.*

[102] *Id.*

[103] MODEL RULES OF PROF'L CONDUCT R. 1.6 (2012).

[104] *See supra* Part I.B.

[105] Perlman, *supra* note 12, at 796.

[106] King, *supra* note 4, at 822.

electronically.[107] This counterargument would be incorrect under the proposed regime because a sending lawyer's lack of reasonable care would need to rise to the level of negligence, as with the test for waiver of confidentiality in inadvertent disclosures within the context of discovery, before waiver of confidentiality could even be considered.

6. Metadata Mining Outside the Context of Discovery Should Be Ethically Permissible Because It Is Allowed Within the Context of Discovery

Although the new FRCP do not specifically address metadata mining, there is a presumption that metadata mining is permissible within the context of discovery due to the potential relevance of the metadata and because ESI, including metadata, is discoverable.[108] There should be no distinction between the situation of two parties in litigation exchanging documents within discovery and the situation of two parties exchanging documents as part of a transactional deal. In both situations, parties should be allowed access to potentially relevant metadata. Furthermore, there should be no distinction between waiver of confidentiality under FRE 502 and waiver of confidentiality in inadvertent disclosures of metadata.

7. Metadata Mining Will Not Significantly Increase the Cost of Legal Services

Some commentators have argued that metadata mining should be ethically impermissible because it will increase the cost of legal services.[109] If metadata mining was prohibited, sending lawyers would not have to bother with ways to limit the transmission of metadata. The concerns in allowing metadata mining are that it will be very costly for sending lawyers to scrub for metadata and receiving lawyers would feel the need to thoroughly mine for metadata to ensure that they uncover all relevant information.[110] These concerns are exaggerated. The cost of metadata scrubbing software is relatively inexpensive and can be as low as a flat $79 per workstation plus an annual maintenance fee that varies as a function of number of workstations and the size of the law firm.[111] As for receiving lawyers, the cost of privilege reviews for the visible parts of thousands of documents is already so high that the cost of a metadata review would be negligible in most cases.[112] Furthermore,

[107] *Id.*

[108] *Id.* at 811–13.

[109] *Id.* at 830.

[110] Perlman, *supra* note 12, at 795.

[111] Israel, *supra* note 20, at 475.

[112] Perlman, *supra* note 12, at 795.

Volume XVI – Fall 2015 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2015.176 ● http://tlp.law.pitt.edu

it would ultimately be in the discretion of receiving lawyers to take the time to review for metadata.

CONCLUSION

Technology has transformed the practice of law within a matter of decades. However, with the ease and efficiency of electronic communications come technologies, such as metadata mining, that can both benefit and harm lawyers. Under the proposed regime of metadata mining, non-confidential information obtained by metadata mining should be ethically permissible outside the context of discovery. Moreover, the use of confidential information obtained by mining outside the context of discovery should be treated like inadvertent disclosures of confidential information within the context of discovery and be ethically permissible when the sending lawyer's duty of reasonable care rises to the level of negligence. Receiving lawyers who mine for metadata are fulfilling their duties of competence and diligence in trying to find information relevant to a client's representation. As long as the duties of sending and receiving lawyers are explicitly defined, the use of non-confidential metadata and certain confidential information obtained by metadata mining outside the context of discovery should be ethically permissible.