

Shannon M. Awsumb, *Avoid Entanglement in Common E-Discovery Pitfalls*, *The Computer & Internet J.*, February 2009, at 27-31.

Electronic discovery (“e-discovery”) has become a key aspect of litigation of all types and sizes and presents a variety of pitfalls that can entrap unwary attorneys who fail to appreciate their responsibilities regarding the search, preservation, production, and receipt of electronically stored information. Failure to successfully navigate e-discovery can result in serious consequences for attorneys and their clients. This article discusses four e-discovery pitfalls and offers suggestions to competently manage these e-discovery issues.

Pitfall # 1. Failing to Conduct a “Reasonable Inquiry” Regarding Electronically Stored Information

One common but easily avoided e-discovery trap involves the failure to properly oversee the production of electronically stored information. Courts are increasingly willing to sanction attorneys for failing to make a “reasonable inquiry” into their clients’ production of electronically stored information during discovery.ⁱ

A recent, widely reported sanctions opinion, *Qualcomm Inc. v. Broadcom Corp.*, highlights the serious consequences attorneys may face when they fail to properly supervise their clients’ production of electronically stored information.ⁱⁱ In *Qualcomm*, during cross-examination at the conclusion of a patent trial, a Qualcomm witness admitted receiving emails that were not produced during discovery. The *Qualcomm* court determined that some of Qualcomm’s attorneys “assisted, either intentionally or by virtue of acting with reckless disregard for their discovery obligations” in Qualcomm’s discovery violations.ⁱⁱⁱ While there was no direct evidence that Qualcomm’s attorneys helped to conceal damaging emails, the court found that the attorneys “contributed” to the

discovery violation because they chose “to accept the unsubstantiated assurances of an important client that its search was sufficient” and ignored warning signs that Qualcomm’s document search and production were inadequate.^{iv} The court imposed considerable sanctions against both Qualcomm and its attorneys because the attorneys did not make a “reasonable inquiry” into Qualcomm’s discovery search and production. In addition to substantial monetary sanctions against Qualcomm, the court referred the sanctioned attorneys to the state bar for investigation and possible sanctions and ordered the attorneys to participate in a comprehensive discovery program to identify the failures in their case management and discovery protocol.

Likewise, in *GTFM, Inc. v. Wal-Mart Stores, Inc.*, Wal-Mart’s attorney represented during discovery that Wal-Mart’s computers lacked the capacity to produce certain electronic records requested by the plaintiffs.^v Deposition testimony later revealed that Wal-Mart’s computers actually had the capacity to produce the requested computer records. The *GTFM* court found that, regardless of whether the attorney’s misrepresentation was intentional, the attorney’s inquiries regarding Wal-Mart’s computer capacity were “certainly deficient.”^{vi} The *GTFM* court sanctioned Wal-Mart by requiring it to pay all plaintiffs’ expenses and legal fees incurred in connection with the inaccurate disclosure of its computer capability and directed an expert of the plaintiffs’ choosing to conduct an on-site inspection of Wal-Mart’s computer facilities at Wal-Mart’s expense.

Courts have made clear that the “reasonable inquiry” requirement puts the burden upon attorneys to reasonably and diligently discharge their obligations to coordinate and oversee e-discovery. Attorneys cannot simply rely on their clients or other third parties

to make a thorough and diligent search for responsive electronic information but must *themselves* supervise and direct electronic discovery efforts. For example, attorneys must take independent action to verify the accuracy and completeness of discovery searches, particularly those conducted by clients' employees or other agents. As one district court explained, attorneys have "a responsibility at the outset of the litigation to 'take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched.'"^{vii} Attorneys cannot simply rely on the fact that a "litigation hold" was put into place at the outset of litigation to satisfy their supervisory obligations because they retain an "on-going responsibility" to ensure that clients have provided all available information and documents responsive to discovery requests.^{viii} Attorneys should actively document their efforts to supervise e-discovery production, including communications with clients and their agents, in anticipation that the reasonableness and thoroughness of the e-discovery process may be later examined by a court.

If attorneys lack the personal knowledge to supervise e-discovery competently and properly, they must take the necessary steps to acquire that knowledge through continuing legal education courses, self-study, or consultation with other attorneys or specialists. As the *Qualcomm* court pointed out, for the "good faith" discovery system to work in the electronic age, attorneys "must take responsibility for ensuring that their clients conduct a comprehensive and appropriate document search."^{ix} Failure to conduct a "reasonable inquiry" into electronically stored information could cause attorneys to violate discovery rules and ethical obligations and thus face considerable sanctions.

Pitfall #2. Relying Upon Improperly Designed or Executed Keyword Searches

Another way attorneys mishandle e-discovery requests is by improperly designing or executing keyword searches.^x In other words, to locate pertinent information on a party's computer, attorneys often work with opposing counsel to establish a process by which to search the computer's database. Problems arise when attorneys fail to understand the consequences and dangers inherent in keyword searches, particularly pertaining to the screening of privileged materials. As one court recognized, e-discovery "presents unique, heretofore unrecognized, risks of waiver of privilege or work-product protection even when the party asserting the privilege or protection has exercised care not to waive it."^{xi}

A faulty searching process can result in a waiver of attorney-client privilege with regard to inadvertently produced documents, as illustrated by the recent opinion in *Victor Stanley, Inc. v. Creative Pipe, Inc.*^{xii} In *Victor Stanley*, the parties agreed on a process to search and retrieve relevant electronically stored information from the defendants' computers. After retrieving responsive documents, the defendants gave their computer experts a list of keywords to use to search and retrieve privileged or protected documents from the set of responsive documents. Later, they discovered that 165 privileged documents had been inadvertently produced to opposing counsel. The *Victor Stanley* court determined that the defendants waived any applicable privilege because they "failed to demonstrate that the keyword search they performed on the text-searchable ESI was reasonable" and that their keyword search was properly designed, supervised, and executed.^{xiii}

Attorneys should understand that “all keyword searches are not created equal” and recognize the risks inherent in relying exclusively on keyword searches to conduct a privilege review of electronic documents.^{xiv} Because even well-designed searches can return unpredictable results, attorneys should carefully test and examine the accuracy of any keyword protocol, particularly with regard to the screening of privileged documents. As the *Victor Stanley* court advised, the “only prudent way to test the reliability of the keyword search is to perform some appropriate sampling of the documents determined to be privileged and those determined not to be in order to arrive at a comfort level that the categories are neither over-inclusive nor under-inclusive.”^{xv}

Attorneys should also consider entering into a “clawback,” “quickpeek” or “nonwaiver” agreement with adversaries prior to any electronic production in order to provide additional protection against claims of waiver.^{xvi} *See also* Fed. R. Civ. P. 26(b)(5)(B); Minn. R. Civ. P. 26.02(f)(2). The *Victor Stanley* defendants chose not to enter into a clawback agreement and instead decided to conduct individualized review of documents.^{xvii}

Finally, attorneys should anticipate that their choice of and execution of the agreed upon process for keyword searches will likely need to be explained and justified in subsequent proceedings (for example, in depositions, evidentiary proceedings, and trials) because even the most carefully planned electronic production can run awry.^{xviii} If attorneys can demonstrate to a court that the process was carefully designed, tested, supervised, and executed prior to the production of electronic documents, a court is less likely to find a waiver of privilege with regard to any privileged documents that may have been inadvertently produced.

Pitfall #3. Exposing Confidential Information to “Metadata Miners”

Attorneys may expose confidential client information to “metadata miners” unless they understand the concept of “metadata mining.” Metadata is simply, “data about data.”^{xxix} Metadata mining refers to the practice of searching for and exploring information embedded in electronic documents. For example, metadata might reveal the author of a document, substantive changes made to a document, hidden text, author comments, the location of the document on a network server, or document versions and revisions.^{xx} While metadata can be innocuous, sometimes metadata will expose a windfall of valuable information that can cause embarrassment or serious consequences to attorneys and their clients.^{xxi}

One high profile example of metadata mining became the focus of litigation involving Merck & Co, Inc.’s painkiller, Vioxx, after *The New England Journal of Medicine* examined hidden tracked changes in a published manuscript for a crucial Vioxx clinical trial.^{xxii} A journal editor was shown a Merck document during a deposition that revealed authors of the Merck study knew of heart problems that were not disclosed in the manuscript submitted to the journal. Following the deposition, the editor and others started analyzing the drafts, raw data and correspondence that Merck provided to the journal years earlier. Their investigation revealed hidden metadata in the draft manuscript that confirmed that Merck researchers knew of the potential cardiovascular side effects of Vioxx years before it was marketed. Further, the metadata showed that Merck had deleted data linking Vioxx to cardiovascular risk just two days before the manuscript was submitted for publication.^{xxiii}

Another high profile incident involved SCO Group’s lawsuit against DaimlerChrysler, which highlights the risks of sharing Microsoft Word or other word processing documents.^{xxiv} Metadata hidden in the Microsoft Word version of a circulated version of the SCO Group’s complaint revealed to the media that before SCO Group filed its complaint, the focus of the lawsuit was not the eventual defendant – DaimlerChrysler – but was actually Bank of America. Shortly before filing, the chosen venue was switched from California to Michigan. The metadata in the complaint also revealed changes to and comments regarding SCO Group’s claims and damages.^{xxv}

From an ethical and practical perspective, metadata found in documents exchanged during discovery is different than metadata mined from documents exchanged outside of the discovery context. During discovery, attorneys may have a duty to produce metadata, though the ultimate production of metadata may depend on the scope of a discovery request and any stipulations made between counsel regarding the production of metadata. Attorneys should not alter or “scrub” metadata from discovery documents, or face likely spoliation sanctions.^{xxvi} Though opinions differ on the ethics of mining for metadata outside of the discovery context,^{xxvii} given the potential to inadvertently provide damaging information about your clients to adversaries, attorneys should exercise caution when sharing electronic documents and take steps to minimize or eliminate the metadata in documents shared outside of the discovery context.

Pitfall #4. Failing To Disclose the Receipt of Inadvertently Produced Documents.

A final e-discovery pitfall involves how attorneys respond when they receive inadvertently disclosed information from opposing counsel or a third party. This

commonly occurs when, for example, an attorney receives a privileged attorney-client communication by error via email.

What are attorneys ethically obligated to do in such a situation? The answer is *not* to lie in wait until the right time comes along to use the document or until opposing counsel discovers his or her error. Minnesota Rule of Professional Conduct 4.4 provides that an attorney “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.*” (emphasis added.) “Document” under Rule 4.4 “includes e-mail or other electronic modes of transmission[.]”^{xxviii} Beyond notification, whether an attorney is required as a matter of law to voluntarily return the document to the sender and to cease from using the document depends on the circumstances. One relevant inquiry is whether the privilege associated with the document has been waived.^{xxix}

While voluntary return of an inadvertently produced document may not be required, it is, more often than not, the professional course to take. One court’s analysis of the issue in *Jones v. Eagle-North Hills Shopping Centre* is insightful.^{xxx} In that case, plaintiff’s counsel inadvertently forwarded a privileged email to opposing counsel and then eight minutes later, immediately requested that defense counsel delete the document. Defendant’s counsel refused to delete the email and attached the email two months later as an exhibit to a pleading. While recognizing that defendant’s counsel committed “no articulable ethical transgression in using the subject email[.]” the *Jones* court commented that the use of the email “could hardly be described as the bell-weather for professional collegiality” and advised that “[e]ven if not driven by a warm feeling of collegiality, such

deference to human fallibility would evince familiarity with the ancient wisdom of ‘What goes around comes around.’ Certainly, such forbearance would be more attuned to the spirit of Model Rule 4.4(b).^{xxxix} In short, while attorneys may not be required to do so, they should thoughtfully consider voluntarily returning inadvertently disclosed documents. When appropriate, they must, at a minimum, notify opposing counsel of the inadvertent disclosure.

Conclusion

Failure to appropriately handle e-discovery may result in serious consequences for both attorneys and their clients. Recognizing the possible pitfalls and understanding the attendant professional and ethical responsibilities can help attorneys avoid personal embarrassment and professional sanctions that may otherwise result. In this day and age, attorneys must understand and competently address e-discovery issues.

ⁱ See Fed. R. Civ. P. 26(g)(2) and Minn. R. Civ. P. 26.07.

ⁱⁱ *Qualcomm Inc. v. Broadcom Corp.*, No. 05-1958, 2008 WL 66932 (S.D. Cal. Jan. 7, 2008), *vacated in part by Qualcomm Inc. v. Broadcom Corp.*, No. 05-1958, 2008 WL 638108 (S.D. Cal. Mar 05, 2008).

ⁱⁱⁱ *Qualcomm*, 2008 WL 66932, at *17. The *Qualcomm* court commented that “[p]roducing 1.2 million pages of marginally relevant documents while hiding 46,000 critically important ones does not constitute good faith and does not satisfy either the client’s or attorney’s discovery obligations.” *Id.* at *9.

^{iv} *Id.* at *13.

^v *GTFM, Inc. v. Wal-Mart Stores, Inc.*, No. 98-7724, 2000 WL 335558, at *1-3 (S.D.N.Y. Mar. 30, 2000).

^{vi} *Id.* at *2.

^{vii} *In re Seroquel Prods. Liability Litig.*, 244 F.R.D. 650, 663 (M.D. Fla. 2007).

^{viii} See *Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc.*, 244 F.R.D. 614, 630 (D. Colo. 2007) (“A ‘litigation hold,’ without more, will not suffice to satisfy the ‘reasonable inquiry’ requirement” because the “obligation to conduct a reasonable search for responsive documents continues throughout the litigation”); *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 432 (S.D.N.Y. 2004) (“*Zubulake V*”) (Scheidlin, J.) (outlining attorneys’ duties to locate, retain and produce information; explaining that a “party’s discovery obligations do not end with the implementation of a ‘litigation hold’ – to the contrary, that’s only the beginning.”).

^{ix} *Qualcomm*, 2008 WL 66932, at *9.

^x A keyword search is a search performed on an electronic database for documents or files containing certain defined terms or keywords.

^{xi} *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 250 F.R.D. 251, 258 n.5 (D. Md. 2008).

^{xii} See *id.*

^{xiii} *Id.* at 262. The *Victor Stanley* court explained that “any order issued now by the court to attempt to redress these disclosures would be the equivalent of closing the barn door after the animals have already run away.” *Id.* at 263.

^{xiv} *Id.* at 256-57.

^{xv} *Id.* at 257. Another district court has similarly advised that “[c]ommon sense dictates that sampling and other quality assurance techniques must be employed to meet requirements of completeness.” See *Seroquel*, 244 F.R.D. at 662.

^{xvi} “Clawback,” “quick peek” and “nonwaiver” agreements generally allow parties to retract documents that were inadvertently produced during discovery. See, e.g., *Hopson v. Mayor and City Council of Baltimore*, 232 F.R.D. 228, 232 (D. Md. 2005) (nonwaiver agreements “protect responding parties from the most dire consequences of inadvertent waiver by allowing them to ‘take back’ inadvertently produced privileged materials if discovered within a reasonable period, perhaps thirty days from production.”). Execution of a detailed clawback agreement can provide greater protection to parties than those set forth in Fed. R. Civ. P. 26 and Minn. R. Civ. P. 26.02, however such agreements are not risk-free. See *Hopson*, 232 F.R.D. at 235.

^{xvii} *Victor Stanley*, 250 F.R.D. at 255.

^{xviii} See *id.* at 261-62 (discussing “best practice points” from *The Sedona Conference Best Practices Commentary on the Use of Search & Information Retrieval Methods in E-Discovery*, 8 Sedona Conf. J. 189, 194-95, 201-02 (Fall 2007)).

^{xix} *Madison River Mgmt. Co. v. Bus. Mgmt. Software Corp.*, 387 F. Supp. 2d 521, 528 n.5 (M.D.N.C. 2005) (metadata “describes ‘how and when and by whom a particular set of data was collected, and how the data is formatted.’”).

^{xx} Brian D. Zall, *Metadata: Hidden Information in Microsoft Word Documents and Its Ethical Implications*, 33 *The Colorado Lawyer* 53 (Oct. 2004).

^{xxi} As the District of Columbia Bar’s Legal Ethics Committee explained, “[t]o the uninitiated, metadata is hidden and perhaps unknown, but to competent computer-users, the existence of metadata is well known and may be a simple ‘click’ or two away.” D.C. Bar Legal Ethics Comm. Op. 341 (Sept. 2007), *available at* http://www.dcbar.org/for_lawyers/ethics/legal_ethics/opinions/opinion341.cfm.

^{xxii} Robert Langreth and Matthew Herper, *Merck’s Deleted Data*, *Forbes.com* (Dec. 8, 2005), *available at* http://www.forbes.com/home/sciencesandmedicine/2005/12/08/merck-vioxxlawsuits_cx_mh_1208vioxx.html.

^{xxiii} *See id.* In November 2007, Merck announced it would pay \$4.85 billion to end thousands of Vioxx suits. *See* Snigdha Prakash and Vikki Valentine, *Timeline: The Rise and Fall of Vioxx*, *NPR.org* (Nov. 10, 2007), *available at* <http://www.npr.org/templates/story/story.php?storyId=16211947>.

^{xxiv} Stephen Shankland and Scott Ard, *Hidden text shows SCO prepped lawsuit against BofA*, *CNET News.com* (Mar. 4, 2004), *available at* http://news.cnet.com/2100-7344_3-5170073.html.

^{xxv} *See id.*

^{xxvi} *See, e.g., Ameriwood Indus., Inc. v. Liberman*, No. 06-524, 2007 WL 5110313, at *1 (E.D. Mo. July 3, 2007) (defendants’ use of scrubbing software to delete computer files and metadata warranted sanctions including entry of default judgment for plaintiff).

^{xxvii} It is not clear whether Minnesota attorneys can ethically “mine” for metadata in electronic documents outside of the discovery context. As of yet, there are no Minnesota decisions or ethics opinions that directly address the issue. Other authorities are split on the issue. *Compare* ABA Formal Op. 06-442 (Aug. 5, 2006) (reviewing and using metadata is permissible); Colo. Bar Ass’n Ethics Comm. Formal Op. 119 (May 17, 2008) (same); Md. State Bar Ass’n Comm. on Ethics, Op. No. 2007-09 (Oct. 19, 2006) (same), *with* Fla. Bar. Ethics Op. 06-2 (Sept. 15, 2006) (metadata mining is impermissible); N.Y. State Bar Ass’n Comm. On Prof’l Ethics Op. 749 (Dec. 14, 2001) (same); Ala. State Bar Ethics Op. 2007-02 (March 14, 2007) (same) *and* D.C. Bar’s Legal Ethics Comm. Op. 341 (Sept. 2007) (review of metadata allowed under certain circumstances).

^{xxviii} Minn. R. Prof. Conduct 4.4, cmt – 2005.

^{xxix} *See id.* Whether attorneys should voluntarily return an inadvertently produced document even when not required by law to do so, is “a matter of professional judgment ordinarily reserved to the lawyer.” *Id.*

^{xxx} *Jones v. Eagle-North Hills Shopping Centre, L.P.*, 239 F.R.D. 684 (E.D. Okla. 2007).

^{xxxi} *Id.* at 686 (granting plaintiff’s motion to strike and remove the privileged email communication from the court file).