Ethical Considerations in Light of the Recent E-Discovery Amendments to the Federal Rules

Electronic communications and devices have changed the way we live and work. As those changes have occurred, litigants and courts have struggled with the application of traditional discovery rules to ever-evolving forms of electronically stored information. On December 1, 2006, several important amendments to the Federal Rules of Civil Procedure took effect. These amendments explicitly modify discovery procedures to address electronically stored information or “ESI.” In particular, the changes impose express obligations on parties to preserve, disclose and produce ESI. While much already has been written about the direct impact of these changes on the discovery process, lawyers must also consider thoughtfully how the recent amendments affect their ethical obligations.

The recent amendments to the Federal Rules impact the ethical obligations of lawyers in a number of respects, but the focus of this Alert is on three such impacts. First, a lawyer’s fundamental duty of competence now extends more clearly to encompass competency regarding electronic technology, including the electronic capabilities of one’s clients. Second, a lawyer’s obligation to act diligently and promptly in representing a client now encompasses the prompt identification and preservation of a client’s electronically stored information. Third, a lawyer’s obligations as the recipient of inadvertently produced privileged documents are heightened by the “clawback” amendments to Rule 26. Each of these areas of increased professional responsibility is further explained and discussed below.

Heightened Competency Requirements

Rule 1.1 of the ABA Model Rules of Professional Conduct (“Model Rules”) requires that “[a] lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation necessary for the representation.”

This competency requirement already has been recognized by the courts as extending to the knowledge, skill, thoroughness and preparation necessary to engage in the discovery of electronically stored information. The recent amendments to the Federal Rules, however, bring into sharper focus the extent to which counsel’s competency requirements now extend to ESI. By these amendments, parties are now obligated (i) even before receipt of a discovery request, to advise opposing parties of the description and location of electronically stored information supportive of its claims or defenses [Fed. R. Civ. P. 26(a)(1)]; (ii) to confer regarding any issues related to the disclosure or discovery of electronically stored information [Fed. R. Civ. P. 26(f)]; and (iii) to appropriately distinguish
between electronically stored information that is reasonably accessible from that which is not [Fed. R. Civ. P. 26(b)]. Moreover, counsel of record shares responsibility with her client for compliance with these obligations [Fed. R. Civ. P. 26(f)].

Several years ago, in a series of groundbreaking decisions in *Zubulake v. UBS Warburg LLC*, District Judge Scheindlin of the United States District Court for the Southern District of New York analyzed, in great detail, discovery obligations related to the production of e-mail records. Judge Scheindlin’s decisions set the standards by which electronic discovery practices, including counsel’s obligations to supervise and monitor discovery, are now often judged; and those standards are incorporated in many respects into the recently amended Federal Rules. With respect to attorney competency, *Zubulake V* made clear that a lawyer’s competency extends to “becom[ing] fully familiar with her client’s document retention policies, as well as the client’s data retention architecture.” This same expectation of competency is now incorporated into the requirements of Federal Rule 26. Thus, lawyers must know how their clients create and use electronically stored information; how they save it; and how it may be deleted or lost – all so that discoverable ESI can be properly disclosed, preserved and produced. This may require extensive investigation by counsel, including interviews of information technology personnel as well as “key players” in the litigation, but there is no longer any question that counsel is obligated to become reasonably knowledgeable about her client’s electronic information and related technology.

A recent decision underscores the considerable risks faced by counsel should they ignore their obligation to be knowledgeable regarding their clients’ ESI. In *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, a Florida state court found that defendant Morgan Stanley had engaged in numerous discovery abuses in connection with e-mail production and imposed one of the harshest sanctions available, *i.e.*, that an adverse inference instruction be read to the jury at trial. Additionally, the court found that Morgan Stanley’s counsel misrepresented the cost of retrieving and producing certain e-mails and allowed false certificates of discovery compliance to be submitted to the court. The court also criticized defense counsel for having “carefully crafted” responses to discovery inquiries so as to avoid disclosure of the existence of certain ESI and to avoid “outright lying.” The court was so disturbed by counsel’s involvement in Morgan Stanley’s “deliberate” and “contumacious” violation of its discovery obligations that it revoked the pror hac vice admission of lead defense counsel.

Lawyers are on notice. Their obligation to provide competent representation in litigation now encompasses reasonable knowledge, skill, thoroughness and preparation regarding a client’s ESI and related technology.

**Heightened Diligence Obligations**

Model Rule 1.3 provides that “[a] lawyer shall act with reasonable diligence and promptness in representing a client.” Additionally, Model Rule 3.4 requires that a lawyer shall not “fail to make reasonably diligent effort to comply with a legally proper discovery request by an opposing party” and shall not “unlawfully obstruct another party’s access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value.” The speed with which electronically stored information is created and altered and the diversity of computer systems and programs used to automatically store and delete such information dramatically impacts a lawyer’s obligations to act diligently with respect to the preservation of discoverable ESI.

---

4 *Zubulake V*, 229 F.R.D. at 432.
5 2005 WL 674885 (Fla. Cir. Ct. 2005).

---

7 *Coleman (Parent) Holdings*, 2005 WL 674885 at *10. In a subsequent proceeding, counsel, by arguing that he was deprived of notice and an opportunity to be heard, was successful in having the revocation of his pror hac vice admission stricken, *Clare v. Coleman (Parent) Holdings, Inc.*, 928 So.2d 1246 (Fla. 2006), but that is small comfort given the trial court’s harsh criticism of counsel’s behavior.
Recently amended Federal Rule 26(b)(1) requires that all potentially relevant evidence, specifically including ESI, be preserved. As explained in *Zubulake IV*, this obligation attaches at the moment a party reasonably anticipates litigation. At that time, the party “must suspend its routine document retention/destruction policy and put in place a ‘litigation hold’ to ensure the preservation of relevant documents.” As further explained in *Zubulake V*, counsel shares in these obligations and is required to:

- Oversee the client’s implementation and compliance with a “litigation hold” designed to preserve all relevant evidence;
- Make certain that all sources of potentially relevant information are identified and placed “on hold;”
- Become fully familiar with the client’s document retention policies, as well as the client’s data retention systems; and
- Take affirmative steps to monitor the client’s production of relevant documents.

The *Zubulake V* court was confronted with the defendant’s failure to preserve a number of relevant e-mail files. The court was extremely critical of both the defendant and its counsel, finding that “counsel failed to properly oversee UBS in a number of important ways, both in terms of its duty to locate relevant information and its duty to preserve and timely produce that information.” Further, the court concluded that while “UBS personnel deleted e-mails, copies of many of these e-mails were lost or belatedly produced as a result of counsel’s failures.” The price paid for these failures was steep. The court imposed sanctions that included an adverse inference instruction with respect to e-mails deleted and irretrievably lost and payment of the costs of any depositions or re-depositions required by the late productions.

The *Zubulake V* court refrained from imposing sanctions upon defense counsel, but defense counsel were not as lucky in *Phoenix Four, Inc. v. Strategic Resources Corp.*, 2006 U.S. Dist. LEXIS 32211 (S.D.N.Y. 2006). In *Phoenix Four*, despite notice of pending litigation, defendants failed to search a number of computer workstations to determine whether they contained information related to the litigation. In seeking sanctions following the late production of ESI amounting to hundreds of boxes of documents, the plaintiff claimed that both the defendants and their counsel had failed to conduct a reasonable and timely inspection of computers and servers in defendant’s possession. The court found both defendants and counsel to have been remiss. With respect to defense counsel’s behavior in particular, the court found that their lack of diligence was “grossly negligent” when they failed to inquire sufficiently of their client regarding the disposition of office computers. The court imposed monetary sanctions that it further ordered were to be borne by the defendants and their counsel equally.

The message is clear. ESI presents unique risks of discoverable information being lost, and these unique risks heighten the diligence required of lawyers to take immediate action to prevent the loss of relevant ESI as soon as litigation arises or is reasonably anticipated.

**Heightened Protection for the Heightened Risks of Inadvertent Production**

Model Rule 4.4(b) requires “[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.” The risk of inadvertent production is heightened in the context of ESI simply because the sheer volume of ESI produced in discovery can be massive. In recognition of this heightened risk, recently amended Federal Rule 26(b)(5) includes a “clawback” procedure for handling inadvertently produced information. By this amendment, a party’s
inadvertent production of privileged information is protected and specific procedures are established for handling such inadvertent productions. For those who are required to produce large quantities of ESI and may have limited time to conduct a thorough privilege review, the “clawback” procedures are an important new protection. Model Rule 4.4(b) and Federal Rule 26(b)(5), however, do not complement each other well, and this is an area where further developments can be expected. For example, in today’s digital environment, a party’s obligations and its counsel’s obligations with respect to metadata are not clear. Metadata is data about data. More importantly, it is usually data that is not apparent on the face of a particular record. Metadata may reflect information about who created a document, who edited it, when changes were made, and what changes were made. Parties who receive records of a type likely to contain metadata are often able to engage in “metadata mining.” What is not clear is whether a party is free to assume that metadata was intentionally produced (and thus is free to “mine” it and take advantage of it) or whether a party must assume that it was inadvertently produced (and thus, if privileged, must return it pursuant to the “clawback” provisions of Federal Rule 26(b)(5)).

Confusing matters further, those states that have considered the ethical implications of metadata mining have reached differing conclusions. The Model Rules contain no specific rules prohibiting it,15 and the Maryland Bar Association has issued an ethics opinion stating that “there is no ethical violation” if a lawyer “reviews or makes use of the metadata without first ascertaining whether the sender intended to include such metadata.”16 In contrast, however, the New York Bar Association has issued an ethics opinion prohibiting lawyers from “mak[ing] use of computer software applications to surreptitiously ‘get behind’ visible documents or to trace e-mail.”17 The Florida Bar Association has reached a conclusion similar to that of New York.18 With respect to metadata, therefore, counsel’s obligations remain either uncharted or dramatically different depending upon which state’s law applies.

Conclusion

As the Zubulake V court cautioned: “Now that the key issues have been addressed and national standards are developing, parties and their counsel are fully on notice of their responsibility to preserve and produce electronically stored information.”19 Counsel’s obligations in this regard derive from their ethical obligations to represent a client’s interests competently and diligently. Those obligations are not new. The world in which they apply, however, has changed dramatically and will continue to do so. Counsel, in order to satisfy their ethical obligations and the newly amended Federal Rules are required to stay abreast of those changes.

16 Maryland State Bar Association, Committee on Ethics, Opinion 2007-092 (November 2006). What remains unclear is whether the Maryland Bar Association would reach a different conclusion if the metadata contained privileged information.
17 New York State Bar Association, Committee on Professional Ethics, Opinion 749 (December 14, 2001).
18 Florida Bar Association, Ethics Committee Opinion 06-02 (September 15, 2006).
19 Zubulake V, 229 F.R.D. at 440.
K&L Gates comprises multiple affiliated partnerships: a limited liability partnership with the full name Kirkpatrick & Lockhart Preston Gates Ellis LLP qualified in Delaware and maintaining offices throughout the U.S., in Berlin, and in Beijing (Kirkpatrick & Lockhart Preston Gates Ellis LLP Beijing Representative Office); a limited liability partnership (also named Kirkpatrick & Lockhart Preston Gates Ellis LLP) incorporated in England and maintaining our London office; a Taiwan general partnership (Kirkpatrick & Lockhart Preston Gates Ellis) which practices from our Taipei office; and a Hong Kong general partnership (Kirkpatrick & Lockhart Preston Gates Ellis, Solicitors) which practices from our Hong Kong office. K&L Gates maintains appropriate registrations in the jurisdictions in which its offices are located. A list of the partners in each entity is available for inspection at any K&L Gates office.

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer.

Data Protection Act 1998—We may contact you from time to time with information on Kirkpatrick & Lockhart Preston Gates Ellis LLP seminars and with our regular newsletters, which may be of interest to you. We will not provide your details to any third parties. Please e-mail london@klgates.com if you would prefer not to receive this information.