SDCBA Legal Ethics Opinion 2012-1
(Adopted by the San Diego County Bar Legal Ethics Committee on November 28, 2012.)

I. FACTUAL SCENARIO

Corporate Client informs Litigation Attorney that it has received a demand letter from a lawyer accusing Corporate Client of specific misconduct and threatening to sue unless Corporate Client ceases the conduct and negotiates a resolution. Corporate Client informs Attorney it does not intend to comply. Attorney gives the issue no further thought.

Three months later Corporate Client informs Attorney that the lawyer who authored the demand letter has sued Corporate Client in federal court alleging the same misconduct identified in the letter. Attorney, while an experienced trial lawyer, is not particularly sophisticated in his understanding or use of digital technology. Attorney accepts the engagement.

II. QUESTION PRESENTED

What conditions, consistent with the California Rules of Professional Conduct and the State Bar Act, must an attorney meet to represent a client in litigation when that client regularly transmits and stores information digitally, including by email?

III. ANSWER

A California attorney may represent a client that regularly transmits and stores information digitally in litigation only if the attorney is reasonably competent in understanding the client's data storage and transmission technology, or professionally consults with another attorney who has the requisite technological competence.[1]

IV. APPLICABLE LAW AND ETHICAL RULES

This opinion analyzes the issue with reference to the Rules of Professional Conduct, Rule 3-110; Rule 3-100; Rule 3-500; Rule 5-200 and the State Bar Act, Business & Professions Code section 6068(d) and (e)(1); ABA Model Rules of Professional Conduct Rule 1.1; 1.6; 4.4; and 5.3 as well as relevant ethics opinions and case law.

V. DISCUSSION

A. A Digital World.

It is hardly a revelation that we now live in a digital world. Today more than 90% of all information is created digitally and 80-90% of that information remains digital. The vast majority of documents containing such information are email. Moreover, 45-50% of stored documents are duplicates or near-duplicates and 85-90% are never referred to after the first

[1] This opinion assumes that the attorney otherwise has the requisite legal skill and learning to represent the client.

transaction. The United States produces well over 50% of the world's digitally stored content each year.[2]

As the cost of digital storage has decreased dramatically, many businesses have concluded that the cost to eliminate unnecessary and out-of-date digitally stored documents vastly outweighs any benefit. As a consequence, the amount of digitally stored information continues to increase exponentially.[3]

Digitally or electronically stored information[4] differs from its analog (paper) predecessor in at least three significant respects. The first is volume. By way of example, a smart phone (16 to 64 GB models) usually have the following equivalent storage capacities: 16 GB, 800,000 to 1.6 million pages; 32 GB, 1.6 million to 3.2 million pages; 64 GB, 3.2 million to 6.4 million pages.[5]

Second, and more importantly, digitally stored information is dynamic. For example, back-up systems "write over" stored data in the preservation process; there are "auto-delete" features available; each email in a string "alters" the original; every time a document is opened, it changes.

Finally, unlike analog documents, some information in digitally stored documents is not apparent (e.g., metadata) but nonetheless exists and can be accessed.

Corporate Client in our facts is no different than any other business; it stores and transmits the vast majority of its information digitally and prints and preserves as paper only a tiny fraction of that information. Moreover, executives at Corporate Client also use laptops, tablets, smart phones and similar devices and many also use "cloud" storage.

B. Rule Changes and Court Decisions.

The obligation in litigation to preserve, gather, screen and produce relevant documents has not changed; nor has the duty to protect a client's confidential information in the process; nor, ultimately, the duty of candor to the court in representing that the lawyer has done so. The almost universal use of digital technology, however, has altered the way lawyers have to address these obligations. This rapid evolution, perhaps revolution, in technology has far out-paced the legal system's recognition that the landscape has changed.

Recent changes in federal and California procedural and discovery rules are attempting to address this new reality.[6] In addition, judicial decisions continue to map the responsibilities of

---

2 San Diego ESI Forum, www.sandiegoesiforum.com, and sources cited there ("ESI Forum").

3 *Id.*

4 Electronically stored information (ESI) is broadly defined as "electronically stored information … stored in any medium from which information may be retrieved" (Fed.R.Civ.P. 34(a)(1)(A)); "information that is stored in an electronic medium" (CCP § 2016.020(e)).

5 ESI Forum, *supra*.

6 The 2006 amendments to the Federal Rules of Civil Procedure identified specifically ESI and, in particular, its preservation, accessibility and sanctions for the failure to preserve and produce it. California's Electronic Discovery Act (2009) modified existing provisions of the CCP to deal specifically with ESI.

clients and attorneys to comply with these new rules.[7] Because of the dynamic nature of digitally stored information, and because relevant information can be irretrievably lost almost in an instant, the obligation to preserve such information as soon as litigation can be reasonably anticipated has become a paramount focus of judicial scrutiny.[8] Critically, judges are becoming increasingly frustrated with parties and their lawyers' failures to meet these obligations and are imposing sanctions, at times serious sanctions, on parties, lawyers or both.[9]

In light of this new reality and the adverse consequences a client could suffer from failure to comply with litigation obligations, this opinion examines whether and in what respects the Rules of Professional Conduct impose new obligations on lawyers in their representation of clients who regularly employ digital data storage and transmission technology.

We conclude that, in litigation, the ethical obligations that a client's regular use of digital technology to transmit and store information implicate in particular are the duties of competence, of confidentiality, of communication and of candor to the courts.

C. The Duty of Competence.

The duty to act competently in the representation of a client is the ethical obligation most directly implicated in the rapid migration to a digital world.

> **Rule 3-110.**
>
> (A) A member shall not intentionally, recklessly, or repeatedly fail to perform legal services with competence.
>
> (B) For purposes of this rule, "competence" in any legal service shall mean to apply the 1) diligence, 2) learning and skill, and 3) mental, emotional, and physical ability reasonably necessary for the performance of such service.

---

7 *Zubulake v. UBS Warburg*, 217 F.R.D. 309 (S.D.N.Y. 2003) (Zubulake I); *Zubulake v. UBS Warburg*, 216 F.R.D. 280 (S.D.N.Y. 2003) (Zubulake III); *Zubulake v. UBS Warburg*, 220 F.R.D. 212 (S.D.N.Y. 2003) (Zubulake IV); *Zubulake v. UBS Warburg*, 229 F.R.D. 422 (S.D.N.Y. 2004) (Zubulake V).

8 *See, e.g., Pension Committee of the Univ. of Montreal Pension Plan v. Bank of America Securities, LLC*, 685 F.Supp.2d 456 (S.D.N.Y. 2010); *Apple, Inc. v. Samsung Electric Co., Ltd.*, 2012 WL 3042943 (N.D. Cal. July 25, 2012). What these cases make clear is that the lawyer now has the obligation to have a documented, repeatable eDiscovery plan and a firm handle on client's technology, business and ESI.

9 For example, *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 2011 WL 2552472 at *2 (D.Md. January 24, 2011) (more than $1 million in attorneys' fees and costs); *Micron Tech., Inc. v. Rambus, Inc.*, 2011 WL 1815975 at *15-16 (Fed.Cir. May 13, 2011); *Hynix Semiconductor, Inc. v. Rambus, Inc.*, 2011 WL 1815978, at *8 (Fed.Cir. May 13, 2011); *Play Visions, Inc. v. Dollar Tree Stores, Inc. No.*, C09-1769MJP (W.D. Wash. June 8, 2011); *Green v. Blitz USA, Inc.*, 2011 WL 806011 (E.D. Tex. March 1, 2011); *In re Delta/AirTran Baggage Fee Antitrust Litig.*, 2012 WL 300509 (N.D. Ga. February 3, 2012); *Conner v. Sun Trust Bank*, 546 F.Supp.2d 1360 (N.D. Ga. 2008) (adverse inference instruction); *In re September 11th Liability Ins. Coverage Cases*, 243 F.R.D. 114 (S.D.N.Y. 2007) (sanction of $1.25 million); *Wachtel v. Health Net, Inc.*, 239 F.R.D. 81 (D.N.J. 2006) (deeming facts admitted, precluding evidence, striking privilege claims, striking trial witnesses, and fine); *Paramount Pictures Corp. v. Davis*, 234 F.R.D. 102 (E.D.P.A. 2005) (spoliation inference).

> (C) If a member does not have sufficient learning and skill when the legal service is undertaken, the member may nonetheless perform such services competently by 1) associating with or, where appropriate, professionally consulting another lawyer reasonably believed to be competent, or 2) by acquiring sufficient learning and skill before performance is required.
>
> ***Discussion:***
>
> The duties set forth in rule 3-110 include the duty to supervise the work of subordinate attorney and non-attorney employees or agents. [Citations omitted.]

1. Expanded Duty of Competence.

Previously, the duty of competence focused primarily on the lawyer's knowledge of the areas of substantive law and the experience necessary to represent the client in the particular engagement. This technology shift has now made that insufficient.[10]

Thus, when representing a client that regularly transmits and stores information digitally in litigation, the "learning and skill" element of Rule 3-110 now also includes understanding the client's technology as well as available preservation, search and review technology. In addition, the lawyer must be familiar with judicial decisions that address specific obligations under either the federal or California rules concerning ESI.

Competence now requires that the lawyer understand his or her obligation to supervise not only subordinate attorneys but also outside vendors whom the proliferation of ESI has spawned, and in addition, his or her obligation also to supervise the client itself, including its executives; the custodians of potentially relevant information; its technologists; as well as any outside vendors whom the client has engaged to assist in the preservation, capture or review of ESI.[11]

---

[10] Accordingly, in August 2012 the American Bar Association amended the ABA Model Rule on competence to address the evaluation of technology: "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice *including the benefits and risks associated with technology*, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject." 2012 Amendment to ABA Model Rule 1.1 Competence, Comment 6, Maintaining Competence. [Emphasis identifies addition.] *See also*, State Bar Formal Opinion 2010-179 the (duties of competence and confidentiality require that an attorney must be able knowledgably to assess the level of security a particular mode of technology affords in order to protect client confidences); New York State Bar Opinion 782 (2004) (reasonable care requires staying abreast of technology advances).

[11] *Cardenas v. Dorel Juvenile Group, Inc.*, 2006 WL 1537394 (D.Kan. 2006). Lawyers have a duty to exercise a degree of oversight over the client's employees to ensure that they are acting competently, diligently and ethically in order to fulfill their responsibility to the court and opposing parties. Trial counsel have obligations to communicate with in-house counsel to identify the persons having responsibility for the matters that are the subject of the document requests and identify all employees likely to have been authors, recipients or custodians of documents falling within the request. Trial counsel also have the obligation to review all documents received from the client to see whether they indicate the existence of other documents not previously retrieved or produced.

2. Sources of ESI.

In an analog world, the location of the client's documents was relatively straightforward: file cabinets at the client's facility(ies); off-site storage; perhaps "working files" at an employee's home. Digital storage capability has dramatically changed that.

Thus, competence begins with an understanding of the sources of the client's ESI—individual desktops, laptops, tablets, smart phones; network hard drives; removable media (e.g., CDs, USB devices); archival data contained on backup tape or other storage media; or cloud storage.[12]

Competence also includes making sure the client (including each custodian) understands the types of evidence that must be preserved: email (sent, received or drafted) and corresponding dates, times, recipients and file attachments; word-processing files; tables, charts, graphs and database files; electronic calendars; proprietary software files; internet browsing applications (bookmarks, cookies, history logs).[13]

3. The Client's Technology.

Next, competence now also means understanding the client's technology: the number, types and locations of computers currently in use and in use during the relevant period if no longer in use; the operating systems and application software the client uses, including the dates of use; the client's file-naming and location/saving conventions; disc-or-tape-labeling conventions; backup and archival disc or tape inventories or schedules; the most likely locations of relevant electronic records; backup rotation schedules and archiving procedures, including any backup programs in use and at any relevant time; electronic-records-management policies and procedures; corporate policies regarding employee's use of company computers and data; and the identities of all current and former employees who have or had access to network administration, backup, archiving or other system operations during the relevant period.

4. Understanding and Issuing a "Litigation Hold."

Precisely because of the dynamic nature of digitally stored information, and the danger of spoliation by routine processes, competence demands that the lawyer instruct the client to issue a litigation hold as soon as there is a "reasonable anticipation of litigation." That anticipation can be triggered by a claim or a demand letter well before suit is filed. Ultimately it is the lawyer's duty to determine whether and when the litigation hold obligation has been triggered.

> Possibly after October, 2003, when *Zubulake IV* was issued, and definitely after July, 2004 when the final relevant *Zubulake [Zubulake V]* opinion was issued, the

---

[12] For example, the New Jersey District Court Local Rule 26.1(d) requires lawyers in that district to review their clients' computer and information management systems "to understand how information is stored and how it can be retrieved" at the very start of the case. The rule sets forth specific procedures for the discovery of digital and computer-based information.

[13] In *Samsung Electronics Co., Ltd. v. Rambus, Inc.*, 2006 WL 20384170 (E.D.Va. 2006) the lawyer's general admonitions to preserve relevant documents was insufficient and the lawyer had to instruct the client on the subject matter and kinds of documents to preserve.

> failure to issue a *written* litigation hold constitutes gross negligence because that failure is likely to result in the destruction of relevant information.[14]

The scope of the written litigation hold is driven by the claims asserted but must cover relevant ESI; relevant custodians ("key players"); sources; and backup and retention programs.

Zubulake V sets out the ethical duties of lawyers in performing in a digital world. The court found that the lawyers had failed their ethical obligations to the client: a litigation hold was insufficient; the lawyer failed to communicate with key players; to monitor compliance; or to locate relevant information. Instead a lawyer must actively monitor the client's compliance with the litigation hold; must become fully familiar with the client's document retention policies, data retention and architecture and electronic systems; must communicate with all key players regarding their ESI storage and retention obligations; and must ensure that relevant backup tapes or other backup media are retained.

To do this, the lawyer must become fully familiar with the client's document retention policies, as well as the client's data retention architecture. This invariably involves speaking with information technology personnel who can explain system-wide backup procedures and the actual (as opposed to theoretical) implementation of the firm's recycling policy. It will also involve communicating with the "key players" in the litigation in order to understand how they stored information.[15]

By far, the most expensive aspect of gathering, screening and producing electronically stored documents is the screening process. Experience is now beginning to demonstrate that "key word" search protocols are the least effective, most time consuming, and most expensive.

Accordingly, competence may also require a lawyer to become familiar with Technology Assisted Review (TAR) or Computer Assisted Review (CAR), or also known as "predictive coding," because of the cost benefit to client and better results.[16]

D. Correlative of Duty of Competence: Duty to Supervise.

A necessary correlative of the duty of competence includes the duty to supervise (*see* the Comment to Rule 3-110 and explicit statement in ABA Model Rule 5.1), including not only subordinates within the lawyer's firm but also non-lawyers both within the firm and outside (*see* ABA Model Rule 5.3). Likewise, subordinates have duties to both their supervisors and the client, the courts and other parties (*see* ABA Model Rule 5.2).

---

[14] *Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities, LLC*, 685 F.Supp.2d 456, 464-465 (S.D.N.Y. 2010) (emphasis in original). Rule 3-110(A): "A member shall not intentionally, **recklessly**, or repeatedly fail to perform legal services with competence." [Emphasis added.]

[15] In *Phoenix Four, Inc. v. Strategic Resources Corp.*, 2006 WL 1409413 (S.D.N.Y. 2006), the court found counsel grossly deficient because the lawyer did not engage in the kind of etiological survey of the client's computers that *Zubulake V* requires. The court also found that the client had an obligation to be aware of *Zubulake IV* and *V*.

[16] *See* Judge Peck's opinion and order in *Da Silva v. Publicis Groupe,* Case No. 11 Civ. 1279 (S.D.N.Y. February 24, 2012).

There are any number of vendors who purport to be "experts" in eDiscovery, some of whom are even non-practicing lawyers. Lawyers representing the client, however, are responsible to supervise not only lawyers and non-lawyers in their own firms but also the outside vendors whom they hire. Accordingly, ultimately the ethical responsibility lies with the lawyer. Thus, the only way an attorney who is not especially competent in the law and practice of eDiscovery can fulfill his or her ethical duty is by taking the time and considerable effort needed to become competent, or by bringing in legal counsel who is competent to assist her or him. Vendors cannot do that.

Accordingly, a lawyer cannot avoid ethical responsibility by "hiring away" eDiscovery to outside vendors who are not lawyers responsible for the client, in spite of the temptation of some vendors to render the equivalent of legal advice. Rather, the lawyer is ultimately responsible both for the vendor's performance as well as the protection of the client's confidential information.

Thus, when the client wants to hire an outside vendor to assist in the eDiscovery process, the lawyer must become involved in the engagement process to ensure that the vendor understands its confidentiality obligations, has the requisite training, understands its duty to scrutinize its work and its obligations in handling confidential information inadvertently produced by other parties.

E. Duty of Confidentiality.

The second ethical obligation digital technology implicates is confidentiality.

California lawyers have an express duty "[t]o maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client."[17] (Bus. & Prof. Code section 6068(e)(1).)

This duty arises from the relationship of trust between a lawyer and a client and, absent the informed consent of the client to reveal such information, the duty of confidentiality has rare exceptions. (Rule 3-100 & discussion ["[A] member may not reveal such information except with the consent of the client or as authorized or required by the State Bar Act, these rules, or other law."].) Rule 3-100 states: "A member shall not reveal information protected from disclosure by Business and Professions Code section 6068, subdivision (e)(1) without the informed consent of the client, or as provided in paragraph (B) of this rule."

ABA Model Rule 1.6 is similar: "A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly

[17] "Secrets" include "[a]ny 'information gained in the professional relationship that the client has requested be held inviolate or the disclosure of which would be embarrassing or would likely be detrimental to the client.'" (COPRAC Formal Opn. No. 1981-58.)

authorized in order to carry out the representation or the disclosure is permitted by paragraph (b)."[18]

1. Implications of Technology and Protection of a Client's Confidential Information.

Because of the volume of digitally stored information and the complexities and cost of the screening process, a lawyer must take special precautions that confidential information is not inadvertently disclosed. Comments 16 and 17 to ABA Model Rule 1.6 (confidentiality) provide some guidance:

> [16] A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Model Rules 1.1, 5.1 and 5.3.
>
> [17] When 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. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.[19]

In this regard, the duty of competence includes taking appropriate steps to ensure both that secrets and privileged information of a client remain confidential—Bus. & Prof. Code § 6068(e)(1) and Rule 3-100—and that the lawyer's handling of such information does not result in a waiver of any privileges.

At a minimum, in any action in federal court, protection of a client's confidential information in the event of inadvertent disclosure may require entering into a stipulation for entry of a protective order as Fed. R. Evid. 502(d) provides. No privilege or protection is waived by disclosure connected with litigation pending before that court—in which event the disclosure is also not a waiver in any other federal or state proceeding. The protection applies, however, only if production of privileged information was an inadvertent disclosure and the client and lawyer

---

[18] The second paragraphs of Bus. & Prof. Code section 6068(e)(2) and Rule 3-100 and ABA Model Rule 1.6 specify the circumstances under which a lawyer may, but is not required to, reveal client confidential information relating to the threat or risk of future harm.

[19] (Model Rule 1.6, comments 16 & 17.)

took reasonable steps to prevent disclosure and took reasonable steps to correct the inadvertent disclosure as soon as the lawyer discovered it.[20]

Metadata, while not apparent, nonetheless exists and can be accessed if it is included with documents produced. Some metadata can reveal client confidential information or strategic decisions in which the lawyer and client participated. Accordingly, the duty to protect a client's confidential information necessarily involves insuring that such information in metadata is not produced.

F. Duty to Communicate with Client.

Digital storage and transmission technology implicates the duty to communicate with the client (Rule 3-500) in very specific ways.

First is the imposition of the litigation hold, both at the outset of the representation, as soon as litigation is reasonably anticipated, and throughout to ensure that digitally stored documents are preserved and collected and produced; it requires communication with the client to identify key custodians and then communicate with those custodians about their preservation obligations.

The duty of communication also includes a candid disclosure to the client at the outset whether the lawyer has the requisite level of technological competence, in addition to all the other lawyering skills and experience, necessary for the engagement and the potential need, at a minimum, to consult with or engage another lawyer with the requisite technological skills.

Zubulake V extends the client's duty to preserve ESI to the attorney. As with other aspects of the representation, this can create a tension between the attorney and the client. For example, if the client chooses not to follow the attorney's advice about how the litigation hold process should be implemented, or information preserved and produced, the possibility for conflict, particularly if a motion for sanctions is filed, is obvious. If a lawyer has a fundamental disagreement with the client, the lawyer may have the obligation to withdraw. Rule 3-700(B).

G. Duty of Candor Toward the Tribunal.

1. Rule 5-200(B); ABA Model Rule 3.3 Require Candor to the Court.

Ultimately, the lawyer will have to represent to the tribunal that the lawyer complied fully with his or her discovery obligations and the consequences for failure to do so can be severe.[21]

Even at the outset of discovery, however, when addressing eDiscovery protocols, candor to the tribunal requires lawyers fairly and accurately to represent what they genuinely believe is necessary—especially in staged discovery—in order to accomplish the principal purpose of discovery: obtain the facts necessary to evaluate, settle or try the case. Accordingly, to argue

---

[20] *See Victor Stanley, supra.* The court found that the defendants waived their privilege on 165 inadvertently produced documents because of the failure to "take reasonable precautions." The defendants used inadequate key words searching and failed to use a quality control process to guard against inadvertent disclosure. The court endorsed The Sedona Conference® Best Practices for search and information retrieval.

[21] See *Zubulake V, supra; Pension Committee, supra; Victor Stanley, supra.*

that, at an absolute minimum, a lawyer needs, for example, 30 custodians and 50 search terms when in fact 15 custodians and 20 terms—especially at the outset—would suffice, a lawyer has not fulfilled her or his duty of candor to the tribunal. In addition, to the extent that the court sees through the persistent, exaggerated demand, a lawyer's incompetence has, arguably, done irreparable injury to the client itself.[22]

Further, while the Rules of Professional Conduct do not have a direct correlate to ABA Model Rule 3.4 (fairness to opposing party and counsel), a court, especially a federal court, might look to the ABA Model Rule for guidance. This rule prohibits unlawfully obstructing another party's access to evidence; concealing a document the lawyer reasonably should know is relevant; making frivolous discovery requests or failing to make reasonably diligent effort to comply with proper discovery requests from an opposing party. Such unreasonableness may be improper under Fed. R. Civ. Proc. 26(g)(1)(B)(ii), triggering a mandatory obligation to impose sanctions.[23]

H. If a Lawyer Does Not Have the Requisite Technological Competence, May the Lawyer Represent the Client?

Rule 3-110 permits a lawyer to represent a client even when the lawyer does not have "sufficient learning and skill" by either (1) associating with or professionally consulting another lawyer reasonably believed to be competent or (2) acquiring sufficient learning and skill before the lawyer has to perform.

Accordingly, the lack of skill in, or experience with, digitally stored and transmitted information is not an impediment to representing a client. But until a lawyer has acquired sufficient skill and learning, the lawyer must either associate or consult another lawyer with the requisite skill for that aspect of the representation, or decline the representation.

I. Application of Ethical Principles to the Facts.

How do these principles apply to the facts set out above?

When Corporate Client informed Attorney of the detailed demand letter from a lawyer threatening litigation, Attorney had the duty seriously to consider whether litigation was reasonably anticipated such that it triggered the obligation to impose a litigation hold even though no suit had yet been filed. Under the facts, Attorney gave no thought to it. As a consequence, during the intervening three months, inevitably electronically stored data has been lost or has been rendered *de facto* inaccessible.

---

[22] In *Magaña v. Hyundai Motor America*, the court found that a defendant—a "sophisticated multi-national corporation experienced in litigation"—improperly limited its discovery search, made false, misleading and evasive responses and willfully violated discovery rules, warranting an $8 million default judgment. 220 P.3d 191 (Wash. 2009); *see also DeGeer v. Gillis*, 755 F.Supp.2d 909, 930 (N.D.Ill. 2010). If the parties had participated in "candid, meaningful discussion of ESI at the outset of the case," expensive and time-consuming discovery and motions practice could have been avoided.

[23] *See Krueger v. Pelican Products Corp.*, Case No. 87-2385-A (W.D. Okla. 1989) (Alley, J.) ("If there is a hell to which disputatious, uncivil, vituperative lawyers go, let it be one in which the damned are eternally locked in discovery disputes with others lawyers of equally repugnant attributes.").

After Corporate Client informed Attorney that it had been sued, Attorney first and foremost had the duty to understand what he did not know about the technology that will be critical to the engagement. Next Attorney must candidly communicate that lack of knowledge and experience to the client before accepting the engagement. Attorney, who under the facts must be presumed not to have the requisite technological knowledge, must immediately consult with another attorney who does. Time is critical because of the absence of an effective litigation hold and the danger of spoliation of relevant information. Absent such consultation, Attorney cannot accept or continue the representation.

VI. CONCLUSION

A California lawyer must either have the technical competence to understand a client's digital data storage and transmission technology, or professionally consult with another lawyer who has the requisite technological competence, in order to represent a client in litigation when that client regularly transmits and stores information digitally.