2-2012

Ethics: The Evils of Email

Lindsay K. Bell

ETHICS: THE EVILS OF EMAIL

Lindsey K. Bell

The Evils of Email

LINDSEY BELL
MILLAR JILES CULLIPHER, LLP
SEARCY, AR

February 24, 2012

I. INTRODUCTION.

A. For better or for worse, email is increasingly the way many people communicate in this era of technology.

B. Forbes – Top Ten Costliest "Smoking Gun" Emails.

C. What's the harm?

1. Lack of context.

a) Facial expression, vocal inflection and body language are not communicated in an email.

b) Messages are easily misconstrued.

2. Litigation.

3. Psychological aspect to email.

II. ATTORNEY-CLIENT PRIVILEGE AND WORK PRODUCT PROTECTION.

A. Attorney-client privilege generally.

1. Protects communications between a lawyer and a client only to the extent that such communications are:

a) Made for the purpose of seeking or providing legal advice, as opposed to business advice;

b) Confidential when made;

c) Kept confidential by the client.

2. The mere fact that an attorney is included in a meeting or on an email does not automatically result in the application of the attorney-client privilege.

C. Work Product Protection.

1. Defined as:

a) Documents or tangible things;

b) That were prepared by or for a party or the party's representative;

c) In anticipation of litigation.

2. Protection from discovery is not absolute.

a) Some courts have held that the "primary purpose" of communication must be legal to be protected. *In re Vioxx*, 501 F. Supp. 2d 789 (E.D. La. 2007).

b) Majority of courts will consider a document to fall within work-product protection if it was prepared "because of" the prospect of litigation. *See U.S. v. Deloitte LLP*, 610 F.3d 129, 137 (D.C. Cir. 2010).

D. Inadvertent disclosure of privileged information.

1. Arkansas Rule of Evidence 502.

a) Inadvertent disclosures do not operate as a waiver if the disclosing party complies with Ark. R. Civ. Pro. 26(b)(5)(A) and notifies the receiving party within 14 calendar days of discovering the inadvertent disclosure by specifically identifying the material or information and asserting the privilege or doctrine protecting it and amending any relevant responses to written discovery.

b) In deciding whether the privilege has been waived, circuit courts will consider:

(1) The reasonableness of the precautions taken to prevent inadvertent disclosure;

(2) The scope of the discovery;

(3) The extent of disclosure; and

(4) The interests of justice.

c) No Arkansas law in the context of electronic discovery, but the Eighth Circuit has endorsed the multi-factor approach recognized in *Gray v. Bicknell*, 86 F.3d 1472, 1483-84 (8th Cir. 1996).

2. Federal Rule of Evidence 502.

a) The new Federal Rule of Evidence 502 was enacted in September 2008 to address cost concerns relating to the production of electronically stored information by creating a presumption against subject-matter waiver and by providing escape routes for inadvertent disclosures of privileged material.

b) Inadvertent disclosures will not waive attorney-client privilege or work-product protection if "the holder took reasonable steps to prevent disclosure" and then "promptly took reasonable steps to rectify the error." Fed. R. Evid. 502(b)(2), (3).

c) The text of the Rule does not define "reasonableness," but the advisory committee notes list the following factors:

(1) The reasonableness of the precautions taken;

(2) The time taken to rectify the error;

(3) The scope of discovery;

(4) The extent of the disclosure; and

(5) The overriding issue of fairness.

E. Company electronic policies and their role in asserting the privilege.

1. Statistics.

   a) 78% of all major US companies keep tabs on employees by checking their email, Internet, phone calls, computer files, or by videotaping them at work.

   b) 63% monitor employees' Internet connections and 47% store and review employee email.

2. Electronic Policy Trumps Privilege.

   a) In *Holmes v. Petrovich Dev. Co*., LLC, 191 Cal. App. 4th 1047 (Cal. Ct. App. 3d Dist. Jan. 13, 2011), personal emails from an employee to her attorney were not protected by attorney-client privilege, as Holmes acknowledged:

      (1) Reading and signing an employee handbook which provided that company computers were to be used only for company business;

      (2) Employees were prohibited from using company computers to send or receive personal email;

      (3) The company would monitor compliance with its computer usage policy and might inspect all files and messages at any time; and

      (4) Employees have no right of privacy for personal information or messages created or maintained using company computers.

   b) *Alamar Ranch, LLC v. County of Boise*, 2009 LEXIS 101866 (D. Idaho Nov. 2, 2009) – Court held that ignorance of an employer's email monitoring policy was insufficient to protect privilege.

   c) *Willis v. Willis*, 914 N.Y.S.2d 243 (N.Y. App. Div. 2010) - Emails to attorney were not privileged where plaintiff's children knew the email password and regularly used the email account, as there was no reasonable expectation of confidentiality in the emails.

3. Company electronic policies can burn unsuspecting lawyers, as well as the employees.Smart lawyers will:

    a) Have their clients call, not email from work.

    b) Be cautious about leaving voicemail messages for clients.

    c) Require clients to use password-protected private email accounts that are secure from third parties only from personal computers.

    d) Never assume that attorney-client email exchanges from a client's work computer are secure even when communications occur through the client's password-protected personal email account.

F. Preservation of privilege.

1. Separate legal advice from non-legal content in distinct communications.

2. Send separate communications to parties who may be protected under attorney/client privilege, such as lawyers and company executives and others.

3. Include specific language such as "counsel is addressing the following legal issues" at the top or bottom of a communication that is intended to offer or solicit legal advice.

4. Mark communications that you want to protect as "confidential" or "privileged" in the subject line, but use judiciously to avoid losing the unique designation.

5. If you think litigation could develop, say that in the communication.

6. Make clear why each recipient is receiving the email.

7. Maintain separate legal and business files where permissible.

    a) *E.I. DuPont v. Forma-Pak*, 351 Md. 396 (1998) – Maryland Court of Appeals denied the applicability

of the privilege to in-house counsel's communications with a collection agency hired to collect a company receivable.

b) Be wary of situations where in-house counsel is performing a business function, not a traditional legal function, in pursuing collection of the corporate debt.

8. Consider adding a "do not distribute, forward or copy this document" directive in the subject line.

III. ETHICS AND ELECTRONIC DISCOVERY.

A. Many times, the information requested from the other side includes all electronically stored information ("ESI") relevant to a particular subject.

1. Arkansas and Federal Rules of Civil Procedure have been amended to include provisions related to the discovery of electronic data.

2. Rules are mandatory for all parties involved in a lawsuit, including all of the parties' employees. These rules apply to everyone.

3. Searching the company server for emails may not be enough if employees also communicate through personal devices, such as iPhones, blackberries, etc.

B. The Sedona Principles.[1]

1. The Sedona Principles were created at the Sedona Conference, which is a nonprofit legal policy research and educational organization comprised of "Working Groups" of judges, attorneys and technologists who are experienced in electronic discovery and document management.

[1]THE SEDONA PRINCIPLES: BEST PRACTICES, RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT DISCOVERY (2d ed. 2007), *available at* http://www.thesedonaconference.org/dltForm?did+TSC_PRINCP_2nd_ed_607.pdf.

2. Places primary responsibility on the parties to confer early.

3. Seeks to reduce costs by requiring parties to properly preserve data, make discovery demands as straightforward as possible and ordinarily limits production to active data unless the requesting party can justify access to back-up data.

4. Cooperation model.

5. Sanctions limited to situations where there has been a clear violation of a duty to preserve evidence, a culpable violation of that duty, and a reasonable probability that the loss of evidence materially prejudiced the adverse party.

C. Traditional concepts apply where the law has not caught up with technology.

1. Competency of counsel.

a) *In re Seroquel*, 244 F.R.D. 650 (M.D. Fla. 2007) – Defendants sanctioned for "purposeful sluggishness." Court recognized Sedona Principle 6.d that that the party and its counsel (and not nonparty consultants or vendors) bear the primary responsibility for ensuring the preservation, collection, processing and production of electronic discovery.

b) Must understand your client's information storage and retrieval system, as well as what information is "reasonably accessible."

2. Duty to make reasonable inquiry.

a) *Qualcomm v. Broadcom*, 2008 U.S. Dist. LEXIS 911 (S.D. Cal. Jan. 7, 2008) – Court awarded Broadcom its attorneys' fees (over $8,500,000) based on Qualcomm's "monumental and intentional" discovery violations.

b) Ultimately, the sanctions were lifted, but the court gave a blistering account of counsel's discovery failures, including:

(1) Counsel chose not to look in the correct locations for the correct documents;

(2) Counsel accepted the unsubstantiated assurances of the client that its search was sufficient;

(3) Counsel ignored warning signs that the document search and production were inadequate; and

(4) Counsel failed to press employees for the truth and/or failed to encourage the employees to provide the information.

3. Duty to preserve.

a) *Rambus, Inc. v. Infineon Techs. AG, Inc*. 222 F.R.D. 280, 288 (E.D. Va. 2004) - Arises the moment that an actual or potential conflict evolves to the point that litigation is "reasonably anticipated."

b) Preservation after a lawsuit is filed is often too late.

c) Assist client in creating a reasonable and realistic policy for preservation as soon as a claim appears likely.

D. What can be retrieved?

1. Basically everything, including:

a) Deleted emails;

b) Fragments of data, even if a portion of the original has been permanently deleted;

c) Instant messaging traffic; and,

d) Internet history and recover images of websites visited.

2. You can run, but you can't hide.

E. Metadata.

1. Data about data.

2. Electronically stored information contains "metadata", which is not a part of the communication usually seen by the sender or recipient.

3. Shows when a document was:

   a) First created;

   b) First edited;

   c) Who created it;

   d) Who edited it;

   e) To whom it was sent and resent;

   f) What was attached to it;

   g) Whether it was a stand-alone email or whether it was part of an email conversation thread; and,

   h) Comments that have been deleted from a previous version.

4. Courts are split on how to handle metadata.

5. ABA Formal Opinion 06-442 does not contain a prohibition against receiving or using metadata and places the burden on the sending lawyer to scrub the data of potentially protected metadata.

F. Consider Proportionality.

1. Must consider the costs of document retrieval and review in comparison to the amount in dispute in the lawsuit.

2. Arkansas Rules of Civil Procedure.

   a) Rule 26.1 was adopted on October 1, 2009.

   b) Rule 26.1 is optional. Either parties agree to comply or the court may order compliance on motion for good cause shown.

c) Electronic information is to be produced in the form in which it is ordinarily kept.

3. Federal Rules of Civil Procedure.

a) Rule 26(b)(2(C)(iii) requires a court to "limit the frequency or extent of discovery otherwise allowed by these rules or by local rule if it determines that the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues."

b) Presumption that the responding party must bear the costs of complying with discovery requests, but courts may shift costs to requesting party based on a proportionality analysis. Fed. R. Civ. P. 26 advisory committee's note (1983).

c) Rule 26(f)(2) requires the parties to discuss at their planning conference "any issues about preserving discoverable information."

(1) During the Rule 26(f) conference, be prepared to say what exists, what will be searched and what will not be searched.

(2) Must still preserve potentially relevant informationeven if initially you do not plan to search it, rely upon it or produce it.

4. Federal Rule of Evidence 502.

a) Consider review protocols.

(1) "Quick peek" protocol – The party responding to a document request produces the documents with no or minimal privilege review, waits for the requesting party to designate the documents it wants for formal production, and then screens the smaller set for privilege and work product protection. *See* Fed. R. Civ. P. 26 advisory committee's note (2006).

(2) "Clawback" protocol – The parties simply agree that production does not lead to waiver so that, if privileged or protected documents are mistakenly produced, the parties need only demand their return. *See* Fed. R. Civ. P. 26 advisory committee's note (2006).

b) Protective Agreements.

(1) Fed. R. Civ. P. 26(f)(3)(D) specifically contemplates protective agreements where the parties agree that they will not claim waiver of privilege or work-product protection against each other if privileged documents are inadvertently produced.

(2) If a federal court enters an order finding that the attorney-client privilege or work-product protection has not been waived by a disclosure with that case, the order is binding in any other state or federal proceeding. Fed. R. Evid. 502(d).

IV. <u>HOW TO KEEP ATTORNEYS IN BUSINESS</u>.

A. Communicate everything by email. Why walk next door?

B. Add as many names to your emails as possible.

C. Don't read before sending.

D. Always reply with your knee-jerk response. Never take time to reflect before sending.

E. Type whatever you want and make sure to include discriminatory or sexual remarks.

F. "Grandmother test" - If a topic is too embarrassing to share with your grandmother, send it anyway!

G. Assume no one is every REALLY going to read your emails. You are an Internet ninja!

H. Be as cagey as possible.

I. Use inappropriate language whenever possible.

J. Longer is better – the more you type, the more words we have to twist around and pull out of context.

K. Keep those chain emails coming.

L. Never check for spelling or punctuation errors. We love any form of evidence showing we are smarter than you!

M. "Reply all" is a lawyer's best friend.

N. Make sure to forward emails containing gossip, hearsay and innuendo.

O. If you're too chicken to say it to someone's face, say it in an email!