fucile & reising | LLP

November 2012 WSBA *Bar News Ethics & the Law* Column

Electronic Update: New WSBA Advisory Opinions on Metadata and Cloud Computing

By Mark J. Fucile
Fucile & Reising LLP

Earlier this year, the WSBA Rules of Professional Conduct Committee issued a pair of advisory opinions providing practical guidance on two emerging areas of "electronic ethics": metadata and cloud computing. The metadata opinion—2216—examines our duties from the perspective of both the sender and the receiver when exchanging documents in electronic form with opposing counsel. The cloud computing opinion—2215—focuses on our responsibilities when using off-site electronic file storage managed by independent vendors. Both opinions are available on the WSBA web site at www.wsba.org.

Core Duties

The metadata and cloud computing opinions revolve around two core duties: competency and confidentiality. RPC 1.1 defines the former and RPC 1.6 the latter.

In the electronic context, the subtitle for Comments 16 and 17 to RPC 1.6 says it all: "Acting Competently to Preserve Confidentiality." We are expected to competently choose methods of electronic file sharing and storage that protect client confidentiality.

Comments 16 and 17 elaborate on both duties:

> "[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 Rules 1.1, 5.1 and 5.3 [the latter two address supervisory responsibilities].
>
> "[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."

These duties are not the simply the province of potential regulatory discipline. Whenever the word "competence" enters the discussion, malpractice risk is sure to follow. Similarly, the Supreme Court in *Eriks v. Denver*, 118 Wn.2d 451, 824 P.2d 1207 (1992), held that the professional rules reflect our underlying fiduciary duties.

Metadata

Lawyers increasingly share documents in electronic form with their opponents in both transactional and litigation contexts. A ready example from transactional practice is a draft contract. An equally ready example from litigation practice is a draft settlement agreement. With electronic file sharing, the concern

is on the "metadata" embedded within the document. The Supreme Court in *O'Neill v. City of Shoreline*, 170 Wn.2d 138, 145, 240 P.3d 1149 (2010), aptly defined metadata as "data about data." Metadata can often reveal, for example, when changes to a document were made, who made them and can include editors' comments. The electronic comments in particular may contain attorney-client communications.

Opinion 2216 looks at metadata from the perspective of both the sender and the receiver. (In doing so, it examines our duties outside the context of formal discovery. Under RPC 3.4, our duties within the context of formal discovery are largely governed by the procedural rules of the forum in terms of what must be produced and what may be withheld.)

From the sender's perspective, Opinion 2216 weaves together the twin duties noted earlier by explaining that we need to sufficiently understand the technology we are using to ensure that we protect confidential material such as attorney-client communications and work product. Opinion 2216 notes that the particular method chosen can vary with the circumstances and will likely change as technology evolves. The options currently available, however, range from transmitting documents in hard copy (or its equivalent, such as fax or mechanically scanned documents) to "scrubbing" software that removes sensitive metadata.

From the receiver's perspective, Opinion 2216 counsels that a lawyer is not prohibited in the first instance from looking at metadata in a document that the lawyer receives from the other side. In many situations, the metadata may be irrelevant because it does not reveal anything of practical value or simply mirrors what the sender intended the receiver to see—such as a "redlined" document. If, however, the metadata contains what appears to be inadvertently produced privileged information, then RPC 4.4(b) directs that the lawyer notify his or her counterpart on the other side. At that point, RPC 4.4(b) leaves to evidence law the question of whether privilege has been waived through inadvertent production and leaves to procedural law the method for litigating potential privilege waiver. These last two points are addressed, respectively, by ER 502 and CR 26(b)(6). Finally, Opinion 2216 generally disapproves specialized "data mining" software that attempts to extract attorney-client communications or work product even if the sender has taken reasonable steps to protect the document involved.

Cloud Computing

Lawyers have used off-site storage for a long time. Traditionally, "off-site storage" meant a physical location (ranging from professionally managed facilities to individual storage units) where lawyers stored their closed files. More recently, "off-site storage" has evolved into "cloud computing" where documents are stored electronically on remote servers managed by independent vendors

and accessed via the Web. Some firms use electronic storage as back-up, some as a primary means of accessing documents and some do both.

The core duties of competence and confidentiality apply with equal measure to electronic storage. The federal district court in Seattle in *In re U.S. Application for a Search Warrant to Seize and Search Electronic Devices from Edward Cunnius*, 770 F. Supp.2d 1138, 1144 n.5 (W.D. Wash. 2011), recently emphasized the role independent vendors play in "cloud computing": "An external cloud platform is storage or software that is essentially rented from (or outsourced to) a remote public cloud service provider[.]" The central involvement of a third party invokes our duty to supervise non-lawyers who assist us under RPC 5.3(a), which requires lawyers and firms to make "reasonable efforts" to make sure that an outside vendor in this circumstance "has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer[.]" In short, a law firm can "contract out" the storage function but not the responsibility for properly acquainting the vendor with a lawyer's duty of confidentiality and receiving reasonable assurance that the vendor has safeguards in place that are consistent with that duty.

Opinion 2215 notes that although lawyers do not need to become computer geeks they at least need to sufficiently understand the technology and safeguards that a vendor uses to make a reasonably informed choice that is in keeping with our duty of confidentiality. The opinion also stresses that these

duties are not static: "Because the technology changes rapidly, and the security threats evolve equally rapidly, a lawyer using online data storage must not only perform initial due diligence when selecting a provider and entering into an agreement, but must also monitor and regularly review the security measures of the provider."

Prudent "due diligence" should also include a review of your firm's insurance coverage for data loss. Oregon's mandatory malpractice carrier (the Oregon State Bar Professional Liability Fund), for example, issued a blanket exclusion for data loss earlier this year. If your firm is not covered, then you will need to balance the utility of off-storage with the corresponding risk. Depending on the type of information stored, statutory law (*see, e.g.,* RCW 19.255.010) may impose requirements for client notification if security is compromised. Imagining yourself writing your clients to inform them about how you lost their sensitive personal information should also be a strong practical motivator for doing "due diligence" on electronic storage providers.

Summing Up

Over the past generation, technology has transformed the practice of law. Electronic file sharing and storage are two prominent examples. The evolution in technology, however, has also produced new challenges for law firm risk management. As the new WSBA advisory opinions highlight, wherever

technology may take law practice, it won't change our bedrock duties to our clients of competence and confidentiality.

ABOUT THE AUTHOR

Mark J. Fucile of Fucile & Reising LLP focuses on legal ethics, product liability defense and condemnation litigation. In his legal ethics practice, Mark handles professional responsibility, regulatory and attorney-client privilege matters and law firm related litigation for lawyers, law firms and legal departments throughout the Northwest. He is a past member of the Oregon State Bar's Legal Ethics Committee, is a past chair of the Washington State Bar Rules of Professional Conduct Committee, is a member of the Idaho State Bar Professionalism & Ethics Section and is a co-editor of the OSB's Ethical Oregon Lawyer and the WSBA's Legal Ethics Deskbook. Mark also writes the monthly Ethics Focus column for the Multnomah (Portland) Bar's Multnomah Lawyer, the quarterly Ethics & the Law column for the WSBA Bar News and is a regular contributor on risk management to the OSB Bar Bulletin, the Idaho State Bar Advocate and the Alaska Bar Rag. Mark's telephone and email are 503.224.4895 and Mark@frllp.com.