fucile & reising | LLP

September 2011 WSBA *Bar News Ethics & the Law* Column

Electronic Ethics, Part 2: Electronic Communication, Metadata and File Storage

By Mark J. Fucile
Fucile & Reising LLP

In our first installment in this series, we looked at social media and law firm web sites. This month, we'll turn to electronic communication, metadata protection when sharing files and electronic file storage. With each, the twin focus is on competently protecting client confidentiality.

Core Duties

RPCs 1.1 and 1.6 outline our duties of, respectively, competency and confidentiality. In the electronic context, the subtitle to Comments 16 and 17 of RPC 1.6 says it all: "Acting Competently to Preserve Confidentiality." We are expected to competently choose methods of electronic communication, 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 vernacular, 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 are reflective of our underlying fiduciary duties.

Communication

The seminal ABA ethics opinion on electronic communication, Formal Opinion 99-413, was issued in 1999 and focused on the "cutting edge" technology of the day: email and cell phones. Although technology has evolved considerably since then, Formal Opinion 99-413 remains relevant for three key reasons.

First, it wove together the twin threads of competency and confidentiality that found their way into the comments to ABA Model Rule 1.6 when revised in 2002 and its Washington counterpart quoted above when amended in 2006.

Second, it concluded that unencrypted email and cell phones were generally acceptable for attorney-client communications because federal law (principally the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2522)

makes the unauthorized interception of those communications illegal, and, therefore, a reasonable expectation of privacy attaches to communications in those forms. The protections afforded by federal law should ordinarily extend to newer variants of both electronic text and voice communications.

Third, the ABA opinion, like Comment 17, counsels that the security measures employed must be balanced against the sensitivity of the information involved. For example, "public" wi-fi sources may not be sufficiently secure for some communications because they are the equivalent of having a discussion in a public place where you may be "overheard."

Metadata

Lawyers increasingly share documents in electronic form with their opponents in both transactional and litigation contexts. A ready example is a draft contract that goes back and forth as parties negotiate toward a final agreement. With electronic file sharing the concern is on the "metadata" embedded within the document. A decision last year under the Public Records Act, *O'Neill v. City of Shoreline*, 170 Wn.2d 138, 145, 240 P.3d 1149 (2010), described metadata as "data about data." Metadata can often reveal, for example, when changes to a document were made, who made them and can also include editors' comments. The electronic comments in particular may contain attorney-client communications.

ABA Formal Opinion 06-442 (2006) looks at metadata from the perspective of both the sender and the receiver.

From the sender's perspective, Formal Opinion 06-442 draws a distinction between documents produced during formal discovery and those simply exchanged during negotiations. On the former, it notes that a producing party may have a duty to include metadata if relevant and requested or to assert any appropriate privilege because ABA Model Rule 3.4(a) (like its Washington equivalent) prohibits lawyers from obstructing another's access to evidence or unlawfully altering or concealing documents. On the latter, it notes the core duties of competency and confidentiality discussed above. Although Formal Opinion 06-442 carefully sidesteps the issues of civil or regulatory liability, it counsels sending documents that might otherwise contain such information in an "imaged" or "hard copy" format (such a scanned "pdf" or simply paper) or "scrubbing" such information (using software designed for this function). Beyond confidential information, Formal Opinion 06-442 notes that virtually all electronic documents that are in their original word processing format (such as Word or WordPerfect) contain a variety of metadata that is not confidential and, therefore, may be shared with the other side.

From the receiver's perspective, Formal Opinion 06-442 predicates its comments with the assumption that the recipient has obtained the document lawfully and, therefore, is not in breach of ABA Model Rule 4.4(a) (which prohibits

gathering evidence in a way that violates the rights of a third party and which is similar to its Washington equivalent). In either a discovery or negotiating context, Formal Opinion 06-442 counsels that a lawyer on the receiving end is not prohibited in the first instance from looking at metadata in a document that the lawyer receives from the other side. If, however, the metadata contains what appears to be inadvertently produced privileged information, then Model Rule 4.4(b) (which is substantively identical in both the ABA and Washington versions) directs that the lawyer notify his or her counterpart on the other side. At that point, both the ABA and Washington versions of RPC 4.4(b) characterize whether privilege has been waived as a question of substantive evidence law rather than a matter of professional ethics. CR 26(b)(6), which became effective last year, outlines the procedural path for bringing potential privilege waiver to the court concerned and ER 502, which also became effective last year, now defines the evidentiary standard for waiver through inadvertent production.

Storage

Just as with paper files, lawyers have an obligation to take reasonable safeguards to protect the confidentiality of electronic files. Unlike paper files, the potential for significant file loss has become much greater as lawyers have moved more of their data to electronic form. For example, although a lawyer might absent-mindedly leave a single paper file at a restaurant following lunch with a client, leaving a "memory key" or laptop loaded with the electronic

equivalent of the lawyer's "file room" presents potential consequences on a much broader scale. The core duties we examined earlier under Comments 16 and 17 to RPC 1.6 apply with equal measure to portable electronic storage. Although encryption or password-protection may not be necessary if otherwise reasonable care is taken to ensure the physical security of a storage device, the measures employed must be balanced against the sensitivity of the information.

Just as paper file storage is sometimes handled by outside contractors, so, too, with electronic storage. This includes "cloud computing," where files are stored on remote servers and can be accessed via the web. Use of outside vendors for file storage has long been permitted and ABA Formal Opinion 08-451(2008) discusses both domestic and international "outsourcing" in detail. With either paper or electronic storage, however, the lawyer or law firm involved remains charged under RPC 5.3(a) with making "reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer[.]" With "cloud computing" in particular, this would include retrieval methods that are sufficiently secure. In short, a law firm cannot "contract out" its responsibility for properly acquainting a vendor with a lawyer's duty of confidentiality and receiving reasonable assurance that the vendor chosen has safeguards in place that are consistent with that duty.

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.