fucile & reising | LLP

July-August 2014 WSBA *NWLawyer Ethics & the Law* Column

Electronic IQ:
Competence in an Era of High-Tech Lawyering

By Mark J. Fucile
Fucile & Reising LLP

Competence is one of our fundamental duties. RPC 1.1 defines competence in the regulatory context to include "the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." The Washington Supreme Court in *Hizey v. Carpenter*, 119 Wn.2d 251, 261, 830 P.2d 646 (1992), described the related civil concept of the duty of care in similar terms: "To comply with the duty of care, an attorney must exercise the degree of care, skill, diligence, and knowledge commonly possessed and exercised by a reasonable, careful, and prudent lawyer in the practice of law in this jurisdiction."

We often associate "competence"—or any shortcomings—with our substantive knowledge of the law. But, office practice failures such as missed deadlines have long been a staple of both regulatory discipline (*see, e.g., In re Lopez*, 153 Wn.2d 570, 106 P.3d 221 (2005) (brief not timely filed)) and legal malpractice (*see, e.g., Huff v. Roach,* 125 Wn. App. 724, 106 P.3d 268 (2005) (underlying action not timely filed)).

Increasingly, our "competence" in both a regulatory and civil sense is also being measured by how we use technology. Particularly as it applies to safeguarding client confidential information, the comments to the confidentiality rule—RPC 1.6—have long woven competence in the selection and use of

technology into our bedrock duty of confidentiality. The ABA's recently adopted "20/20" amendments to its influential Model Rules that are under review in Washington also include the notion of staying current with new technology as a central element of our duty of competence. In this column, we'll survey first our duties of "electronic" competence and then use electronic file storage as a practical example.

Before we do, however, two important qualifiers are in order. First, in the regulatory context, not every instance of negligence automatically implies a lack of competence under RPC 1.1 (*see In re Anschell*, 141 Wn.2d 593, 609 n.4, 9 P.3d 193 (2000)). Second, in the civil context, any asserted negligence must have caused the damages sought to support a claim for legal malpractice *(see Daugert v. Pappas*, 104 Wn.2d 254, 257-63, 704 P.2d 600 (1985)).

Electronic Competence

Newly revised Comment 18 to ABA Model Rule 1.6 neatly summarizes the interplay between competence and confidentiality:

> "*Acting Competently to Preserve Confidentiality*
>
> "Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and 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 unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the

> sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use)."

The current version of Washington Comment 16 to RPC 1.6 is similar and the new ABA formulation is under review here.

The ABA Model Rule amendments also include an explicit tie between competence and keeping current with new technology in Comment 8 to Model Rule 1.1:

> "*Maintaining Competence*
>
> "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 relevant technology[.]"

The current version of Washington Comment 6 to RPC 1.1 discusses continuing education generally, but does not have the explicit tie between competence and new technology. This new ABA formulation, however, is also under review here.

Example: Electronic File Storage

Although technology has transformed many aspects of law practice, one of the best illustrations is file storage. Paper files are gradually giving way to various forms of electronic storage—ranging from local media to remote "cloud" services. The ability to store and retrieve data seamlessly both within and outside our offices affords many benefits for lawyers and clients alike.

At the same time, the consequences of data loss or theft are potentially more far reaching as well. In years past, a paper file inadvertently left behind at a restaurant after lunch with a client raised potential confidentiality issues if not recovered quickly—but they were normally limited to the single client concerned. By contrast, a laptop left behind at that same restaurant today may magnify the confidentiality issues across the lawyer's entire client base if the computer holds the lawyer's "virtual file room." Similarly, the theft of a law firm's confidential information through "hacking" into its servers—whether on-site or maintained remotely—can present those issues even more starkly.

Beyond the RPCs, many states, including Washington (*see* RCW 19.255.010), have broad data breach notification laws.

The federal district court in Seattle commented on both the rise of electronic data theft and related litigation in *Krottner v. Starbucks Corp.*, 2009 WL 7382290 at *2-*3 (W.D. Wash. Aug. 14, 2009) (unpublished; citations omitted):

> "Digital collections of thousands or even hundreds of thousands of people's personal data are ubiquitous, and theft or loss of those collections is, if case law is any indication, becoming increasingly common. In some cases, information is compromised by hacking into computer networks that store personal information . . . Often, as in this case, plaintiffs raise claims arising from the theft of computers that contain collections of personal information.
>
> "Accompanying the rise in the theft or loss of such data collections is a rise in civil suits. The theft or loss of a data collection brings with it the possibility of what the court will broadly refer to as 'indentify theft.' In the hands of an identity thief, a plaintiff's personal information can be used to gain access to his financial accounts, open new accounts in his name, and engage in other schemes limited only by the thief's ingenuity."

The WSBA in Advisory Opinion 2215, which was issued in 2012, discussed the general factors that lawyers should consider in evaluating cloud computing services. Although remote storage presents some unique issues precisely because we are using an independent vendor often operating at significant physical distance from our office, much of the advice rings true even for storage that is located closer to (or in) our offices. Advisory Opinion 2215 also echoes the comments noted in weaving together the concepts of competence and confidentiality:

> "A lawyer using such a service must, however, conduct a due diligence investigation of the provider and its services and cannot rely on lack of technological sophistication to excuse the failure to do so. While some lawyers may be able to do more thorough evaluations of the services available, best practices for a lawyer without advanced technological knowledge could include:
>
> "1. Familiarization with the potential risks of online data storage and review of available general audience literature and literature directed at the legal profession, on cloud computing industry standards and desirable features.
>
> "2. Evaluation of the provider's practices, reputation and history.
>
> "3. Comparison of provisions in service provider agreements to the extent that the service provider recognizes the lawyer's duty of confidentiality and agrees to handle the information accordingly.
>
> "4. Comparison of provisions in service provider agreements to the extent that the agreement gives the lawyer methods for retrieving the data if the agreement is terminated or the service provider goes out of business.
>
> "5. Confirming provisions in the agreement that will give the lawyer prompt notice of any nonauthorized access to the lawyer's stored data.

"6. Ensure secure and tightly controlled access to the storage system maintained by the service provider.

"7. Ensure reasonable measures for secure backup of the data that is maintained by the service provider."

Finally, Advisory Opinion 2215 notes that our duties don't end with selection of a service. It counsels that because technology changes rapidly, lawyers "must also monitor and regularly review the security measures of the provider."

Summing Up

Lawyers don't necessarily need to become "computer nerds" to meet their duty of competence if we have sufficient internal or external technical assistance. But, any lawyer using technology has to understand it well enough to meet our many responsibilities to our clients—including our fundamental duty of 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 NWLawyer (formerly 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.