RISK OVER SUBSTANCE

The Escalating Risk of The Practice of Law Under Ethics Rules Related to Technology

By Danny M. Howell, Esq.
Law Offices of Danny M. Howell PLLC

The complexities of the practice of law are increasing geometrically, the Courts' appetite for facilitating legal malpractice claims is robust, and the panoply of government agencies that enforce legal ethics requirements – the state bars, the SEC, the Patent & Trademark Office, the U.S. Trustee, and the Courts themselves – becomes more aggressive by the day. The often crushing costs of defending malpractice suits, ethics investigations and bar proceedings impact all of us through higher insurance premiums. For attorneys without insurance coverage, a single malpractice suit or bar proceeding can lead to bankruptcy, together with harsher sanctions due to the inability to pay for a defense.

Remember the old Steve McQueen movie "The Blob"? The profession increasingly finds itself backpedaling due to an ever-expanding application of the ethics rules, such as new requirements of "technological competence," the transmogrification of acts of negligence into findings of incompetence under Rule 1.1 of the Model Rules,[1] and the metastasizing application of the "conduct unbecoming" provisions of Rule 8.4 to actions unrelated to the practice of law, which together with enforcement methods that are increasingly aggressive, have turned the career paths of attorneys into a trip around a Monopoly board.

And all of this is built upon the foundation of a set of legal ethics rules so full of vague buzzwords that the answer to the question of precisely what they mean often requires consulting the Oracle.

There are, of course, many clear instances of misconduct that rightfully lead to punishment; and there are devoted professionals engaged in the enforcement of the ethics rules. But the vagaries in the rules themselves can lead to uneven application. Moreover, given the increasing costs of defense against ethics proceedings, the impact of ethics enforcement likely falls disproportionately on

---

[1] All references to the Rules refer to the American Bar Association (ABA) Model Riles of Professional Conduct.

sole practitioners and small firms, which simply cannot afford the hundreds of thousands of dollars required to defend a serious set of ethics charges.

Let's visit a few areas of growing risk:

RULE 1.1's NEW REQUIREMENT: TECHNOLOGICAL COMPETENCE

Rule 1:1 still states, in ethics buzzword-ese, the same general requirement of "reasonably necessary" competence:

> *"A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."*

However, in 2012 the ABA approved a new addition to comment 8 to Model Rule 1.1: "*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****, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."*

This comment is, like many of the Rules themselves, written in such a general way as to be mush. What is "relevant technology"? Moreover, presumably the lawyer has to **understand** the technology to a certain extent (although undoubtedly with an expert's assistance) – but how much is required?

In addition, the comment is incredibly broad, encompassing such things as computer and e-mail hacking, and encryption of documents created or transferred electronically.

But the most dangerous risk associated with technology involves electronic document destruction; and the comment gives additional incentive to Courts looking to impose huge sanctions on lawyers who fail to stop clients' document routing destruction of electronic documents.

Lawyers are now even required to police the compliance of clients with "litigation hold" letters. See Browder v. City of Albuquerque, 2016 U.S. Dist. LEXIS 76397 (D.N.M. May 9, 2016) ("**Counsel . . . have a continuing**

responsibility to ensure that the parties preserve relevant information * * *. This responsibility obligates counsel to do more than simply notify all employees of a litigation hold and expect that the party will then retain and produce all relevant information. Counsel must go beyond mere notification and take affirmative steps to monitor compliance," to talk to key employees in an effort to understand how evidence will be stored**, to continually ensure that the party is preserving relevant evidence."**) (internal citation and punctuation omitted).

As a result, even small practices must incur the expense of yet another type of insurance policy -- cyber insurance. The policies vary greatly in language (and thus in what is or isn't covered), but they are fast becoming essential protections against charges we may face based upon the over-reaching language of Comment 8.

This responsibility imposes potentially huge costs on firms – costs that might not be able to be passed on, or passed on fully, to the client since, ostensibly, the obligation to "monitor compliance" is an ethical duty that exists regardless of whether the client asks the attorney to do it or agrees to pay for it. See In re Lawyers Professional Responsibility Bd. Panel No. 94-17, 546 N.W.2d 744, 747 (Minn. 1996) ("[A]ttempting to charge any fee for time spent responding to a client's charge of unethical conduct is inherently unreasonable and violates Minn. R. Prof. Conduct 1.5(a), which provides that a lawyer's fee shall be reasonable.").

The duty to "ensure" compliance arguably makes the attorney a guarantor of the client's compliance. In larger cases, even the IT department of a large firm may be ill-equipped to handle such a task. The prospect of huge sanctions for non-compliance has caused a cottage industry of e-discovery companies to spring up, increasing the cost of litigation while presumably imposing another layer of monitoring obligations upon counsel, who now also have to "ensure" that the consultant firm does its job properly, too.

RULE 1.4 COMMUNICATION

Encryption

Not properly protected, laptops and portable media can be recipes for a security disaster. One survey reported that 70 percent of data breaches resulted from the loss or theft of off-network equipment (laptops, portable drives, PDAs, and USB drives). Strong security is a must. Encryption is now a standard security measure for protecting laptops and portable devices—and attorneys should be using it.

David G. Ries and John W. Simek, *Encryption Made Simple for Lawyers*, GPSOLO, Vol. 29, No. 6 (Nov./Dec. 2012)[2]

Flowing from the technological competency issue above, lawyers are increasingly likely to find that they have a duty to encrypt electronically transmitted communications as an unrelenting wave of hacking and related computer fraud hits our industry.

ABA Formal Opinion 99-413 states that "a lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the Model Rules of Professional Conduct," but "a lawyer should consult with the client and follow her instructions, however, as to the mode of transmitting highly sensitive information relating to the client's representation." Moreover, ABA Formal Opinion 11-459 requires lawyers to warn client of e-mail risks where there is a significant chance that third parties, such as employers, will gain access to them.

In addition to ethical duties, Nevada and Massachusetts have enacted statutes broadly affecting any business that transmits personal data electronically (including by e mail) – or, in Nevada's case, that merely stores such information on a laptop that is taken off the business premises – and requiring those businesses to encrypt the personal information. See C. Kennedy, "Complying with Personal ID Encryption Mandates," Iron Mountain White Paper (2010), available at

---

[2] Available at: http://www.americanbar.org/publications/gp_solo/2012/november_december2012privacyandconfidentiality/encryption_made_simple_lawyers.html.

http://www.ironmountain.com/Knowledge-Center/Reference-Library/View-by-Document-Type/White-Papers-Briefs/C/Complying-with-Personal-ID-Encryption-Mandates.aspx (last visited April 21, 2016).

To a certain extent, attorneys can solve certain technology security issues through use of services that encrypt e-mail and document transfers, like Dialawg, Rpost or ZixCorp.

When documents have to be reviewed quickly by the client, and e-mailing multiple versions gets too confusing, one solution is to use a secure online repository such as ShareFile – you upload the documents, and the client uses a password to access them securely.

The article *Encryption Made Simple for Lawyers*, supra, contains an extensive discussion of encryption methods for laptops, smartphones and tablets, wireless internet, and e-mail.

What is the response to all of this? There are a number of cyberfraud-related insurance policies and supplemental coverages available -- these are non-standard policies so their provisions bear careful review, but having such coverage might be increasingly necessary today, especially for practices that receive electronic records most dear to hackers' hearts -- social security and bank account information, wiring instructions, etc.

In the meantime, don't be surprised if the standard for compliance becomes one that is affordable by large firms, and not so much by solo and small practices. There may be only one set of ethics rules, but it ought to be flexible enough to acknowledge the differences in resources between large and small practices in complying with technology requirements.