fucile & reising | LLP

April 2019 Oregon State Bar Bulletin

From Beginning to End: Risk Management Over the Life Cycle of Technology

By Mark J. Fucile
Fucile & Reising LLP

Twenty years ago the ABA released a seminal ethics opinion on a lawyer's duty of confidentiality when using technology. Although the principles underlying that opinion remain as central to law practice today as they were in 1999, technology itself has changed radically. The 1999 ABA opinion was framed around "cordless" telephones, fax machines and email services such as CompuServe. Those illustrations highlight a key element of law firm risk management when it comes to technology: because technology is continually changing and being replaced, we need to approach risk management over the entire life cycle of the services and devices involved. In this column, we'll first survey basic risk management principles applicable to all law firm technology and then turn to three phases in the technological life cycle: (1) selection; (2) use; and (3) disposal.

Basic Principles

Lawyers have a fundamental duty to protect client confidentiality. The Ninth Circuit has described confidentiality as one of a lawyer's most "basic" fiduciary duties.[1] This duty is reflected squarely in our regulatory requirements under RPC 1.6. Statutory obligations can also enter the mix. ORS 9.460(3), for

example, requires attorneys to "[m]aintain the confidences and secrets of the attorney's clients consistent with the rules of professional conduct[.]"

At the same time, the duty imposed is not unlimited. Oregon RPC 1.6(c), which is patterned on its ABA Model Rule counterpart, tells us that "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

Even tempered with the word "reasonable," the consequences of a lawyer or law firm's failure to meet the duty of confidentiality can be both severe and several. Oregon lawyers have been suspended for failure in their regulatory responsibilities under the confidentiality rule.[2] Comments 18 and 19 to ABA Model Rule 1.6 emphasize that meeting our confidentiality obligations is a part of our equally basic duty of competent representation under Rule 1.1. Although the regulatory duty of competence is not synonymous with the civil standard of care, it doesn't take much imagination to envision a legal malpractice or breach of fiduciary duty claim arising from a confidentiality failure. Moreover, our duties may extend beyond clients depending on the kind of information a law firm is holding. The Oregon Consumer Identity Theft Protection Act, for example,

includes reporting obligations in the event of a security breach involving specified personal information to affected "consumers" who may—or may not—be clients.[3]

Selection

Law firm risk management on the technology front begins with the selection of services and devices. Comment 8 to ABA Model Rule 1.1 emphasizes that lawyers must understand the technology they use. This doesn't mean that lawyers must get masters' degrees in computer science. It does mean, however, that we may need to obtain sufficient technical help to assist us in selecting technology that meets our duty of confidentiality. Oregon State Bar Formal Opinion 2011-187 (rev 2015), which discusses metadata in electronically-exchanged documents, notes that competency "requires a lawyer utilizing electronic media for communication to maintain at least a basic understanding of the technology and the risks . . . or to obtain and utilize adequate technology support."[4] Larger firms typically have this expertise in-house with their IT staffs. Smaller firms, by contrast, often use independent consultants in this advisory role. Whatever the approach, lawyers are not allowed to simply "plead ignorance."

Oregon State Bar Formal Opinion 2011-188 (rev 2015), which focuses on cloud services, outlines general factors lawyers should consider when evaluating services in particular:

> "Under certain circumstances, . . . [compliance with RPC 1.6(c)] . . . may be satisfied through a third-party vendor's compliance with industry standards relating to confidentiality and security, provided that those industry standards meet minimum requirements imposed on the Lawyer by the Oregon Rules of Professional Conduct. This may include, among other things, ensuring the service agreement requires the vendor to preserve the confidentiality and security of the materials. It may also require that vendor notify Lawyer of any nonauthorized third-party access to the materials. Lawyer should also investigate how the vendor backs up and stores its data and metadata to ensure compliance with the Lawyer's duties."[5]

Formal Opinion 2011-188 also notes that selection criteria is not frozen in time:

> "Although the third-party vendor may have reasonable protective measures in place to safeguard the client materials, the reasonableness of the steps taken will be measured against the technology. . . Accordingly, Lawyer may be required to reevaluate the protective measures used by the third-party vendor to safeguard the client materials."[6]

Use

Using technology in keeping with our duty of confidentiality involves a blend of physical and electronic security.

Physical security often means simply using the protective measures now commonly built into most devices. For example, devices should routinely be

password protected and hard drives encrypted. Because mobile devices in particular can be stolen notwithstanding reasonable care, remote "kill switches" that are now also common in many mobile platforms should be activated so that a stolen device can be "wiped" or otherwise rendered inoperable remotely.

Electronic security has "outbound," "inbound" and "static" components.

On the "outbound" side, ABA Formal Opinions 99-413 (1999) and 477R (2017) emphasize that a lawyer is responsible for choosing a method of communication that is commensurate with sensitivity of content involved. A coffee shop's free public wi-fi, for example, might be appropriate for a quick email back to an assistant to confirm a routine meeting but not for a strategy discussion with a client about a not-yet-announced corporate merger proposal. Although neither ABA opinion requires encryption in light of federal statutory law prohibiting the unauthorized interception of electronic communications, the increasing availability of encryption means that it is at least another tool to be evaluated in determining the method of communication chosen.

On the "inbound" side, ABA Formal Opinion 11-459 (2011) reminds lawyers that they are responsible for educating clients on the ramifications that the use—or misuse—of technology may have on the attorney-client privilege. A lawyer handling a hotly contested divorce, for example, might prudently advise a

client on the potential loss of privilege by using an employer's computer to communicate sensitive information to the lawyer.

Finally, as for "static" storage, lawyers remain responsible for taking reasonable measures to safeguard their increasingly electronic files. Just as a law firm would not let strangers wander around its paper file room, a firm can't do the same with its electronic files. An Oregon lawyer was disciplined, for example, for storing client files from his part-time law practice on a State computer at his full-time job as a State employee that were then accessed by his State supervisor when the lawyer left his State job.[7]

Disposal

With the pace of technological change, law firms today are continually replacing old systems and devices with their newer counterparts. Many of those old devices contain sensitive client information. Oregon State Bar Formal Opinion 2005-141 (rev 2015) addresses recycling paper documents but its advice is equally apt for electronic storage on devices that are being replaced:

> "Oregon RPC 1.6(c) requires lawyers to take reasonable efforts to prevent inadvertent or unauthorized access. As long as Law Firm makes reasonable efforts to ensure that the recycling company's conduct is compatible with Law Firm's obligation to protect client information, the proposed contract is permissible. Reasonable efforts include, at least, instructing the recycling company about Law Firm's duties . . . and obtaining its agreement to treat all materials appropriately."[8]

In addition to commercially available software programs to "wipe" devices clean, the Professional Liability Fund has information on its web site about local electronics recyclers that securely destroy hard drives and their equivalents and then dispose of non-reusable components in an environmentally responsible way. Cloud services used should also have described protocols for permanent deletion of stored files if a law firm changes vendors and files have been transferred to a new service.

Summing Up

Confidentiality is one of our oldest duties. Ironically, technology has made confidentiality more cutting edge than ever. It is a duty that follows from beginning to end over the life of the technology we use in law practice. We need to approach our risk management accordingly.

ABOUT THE AUTHOR

Mark J. Fucile of Fucile & Reising LLP handles professional responsibility, regulatory and attorney-client privilege issues for lawyers, law firms and corporate and governmental legal departments throughout the Northwest. Mark has chaired both the WSBA Committee on Professional Ethics and its predecessor, the WSBA Rules of Professional Conduct Committee. Mark is also a former member of the Oregon State Bar Legal Ethics Committee and is a current member of the Idaho State Bar Section on Professionalism & Ethics. Mark writes the monthly Ethics Focus column for the Multnomah (Portland) Bar's *Multnomah Lawyer*, the quarterly Ethics & the Law column for the WSBA *NWLawyer* and is a regular contributor on legal ethics to the WSBA *NWSidebar*

blog. Mark is a contributing author/editor for the current editions of the OSB Ethical Oregon Lawyer, the WSBA *Legal Ethics Deskbook* and the WSBA *Law of Lawyering in Washington*. Before co-founding Fucile & Reising LLP in 2005, Mark was a partner and in-house ethics counsel for a large Northwest regional firm. He also teaches legal ethics as an adjunct for the University of Oregon School of Law at its Portland campus. Mark is admitted in Oregon, Washington, Idaho, Alaska and the District of Columbia. He is a graduate of the UCLA School of Law. Mark's telephone and email are 503.224.4895 and Mark@frllp.com.

---

[1] *Parker Drilling Company v. Hughes, Thorsness, Gantz, Powell & Brundin*, 1997 WL 469644 at *1 (9th Cir Aug 18, 1997) (unpublished).

[2] *See, e.g., In re Lackey*, 333 Or 215, 37 P3d 172 (2002) (one-year suspension); *In re Huffman*, 328 Or 567, 983 P2d 534 (1999) (two-year suspension).

[3] *See* ORS 646A.600, *et seq*. ABA Formal Opinion 483 (2018) addresses related ethical duties in the event of a data breach.

[4] *Id*. at 2-3.

[5] *Id*. at 3-4 (citation omitted).

[6] *Id*. at 4-5 (citation omitted).

[7] *In re Valverde*, 29 DB Rptr 192 (Or 2015).

[8] *Id*. at 3.