BAR BULLETIN

KCBA KING COUNTY BAR ASSOCIATION

Justice... Professionalism... Service... Since 1886

*This is a reprint from the King County Bar Association Bar Bulletin*

December 2015

# Online Document Reviews — Crossing an Ethics Line?

***By Larry G. Johnson***

A major development in e-discovery is for law firms to let third-party vendors collect and process their clients' electronically stored information (ESI), then host it online "in the Cloud" so various members of the litigation team regardless of location can access the documents for privilege and relevance reviews. While this use of the Internet provides a convenient way to manage and divide labor, if you go that route, have you considered the risks involved in terms of possible ethics violations or potential malpractice claims?

There have been so many cases of spectacular computer hacks in the news lately (e.g., Target, T-Mobile, federal employees' data), how do law firms think they can do any better in keeping confidential client information secure when allowing their clients' data to be hosted online for document reviews?

## The Ethics Basics

Before discussing how you can limit your risks in handling and housing your clients' ESI, let's look at what the Rules of Professional Conduct expect of you, and where you might even run afoul of a law you may not have fully appreciated that applies to you as well as your client (e.g., HIPAA, if you have health care industry clients, or FERPA, which covers student records confidentiality for schools/school districts and those who represent them).

The relevant RPCs that apply to online data risks are the following:

> RPC 1.1, 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.
>
> RPC 1.6, CONFIDENTIALITY OF INFORMATION: (a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

"Competence" as understood in RPC 1.1 includes knowledge about your clients' computer and information management systems, and that includes a minimum ability to engage in a proper communication and liaison with the IT and records management people. The days of lawyers gleefully proclaiming computer ignorance ("Hey, I can't even tell you where the F1 key is!") are over.

If you think you lack tech-savvy to talk intelligently about your clients' ESI with their employees entrusted with that information, then you need to obtain the services of an expert to do that for you, or who can advise and educate you so you can. If there was ever any doubt about that, it was amply laid to rest in WSBA Advisory Opinion 2215,[1] which directly deals with the "ethical obligations related to the use of online data storage managed by third party vendors to store confidential client documents."

Here is the meat of Opinion 2215:

> A lawyer using [a third party service provider of online data storage] 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.
>
> A lawyer has a general duty of competence under RPC 1.1, which includes the duty "to keep abreast of changes in the law and its practice." RPC 1.1 Comment 6. To the extent that a lawyer uses technology in his or her practice, the lawyer has a duty

to keep informed about the risks associated with that technology and to take reasonable precautions.

So, on a scale of 1 to 10, how do you fare in meeting those criteria? And, not to put too fine a point on it, just how do you know you know? Paraphrasing our former Secretary of Defense Donald Rumsfeld, a big problem for lawyers, as for anyone else, is "not knowing what you don't know."

Of course, the RPCs discussed above not only define the appropriate professional conduct, they also establish evidence of the standard of care toward clients that is expected of lawyers, so these RPCs' relationship to possible malpractice claims is rather obvious.

## Other Potential Sources of Liability

And just to add a little more moisture to your armpits: What if you happen to have a client's health care information hosted online and that gets hacked or leaked, what is your potential liability specific to that kind of information? If your client is in the health care industry, another bar publication, this one from Tennessee,[2] gives this scary answer by way of a hypothetical:

> After copying the medical records of almost 600 patients to a personal flash drive, you ask your assistant to deliver the records to a billing consultant. But your assistant has dinner plans, so she drops the flash drive in her purse, intending to deliver it before work the next day. Unfortunately, your assistant forgets her purse at the restaurant. The purse and the flash drive are never recovered.
>
> So what would this mean for your firm? Your client, likely your former client now, must contact each of the affected patients, publish notice of the incident in the media, and notify HHS. Additionally, your client may seek reimbursement from your firm for any government fines and the substantial costs it incurred in sending the notifications and hiring new counsel to advise it on the incident. Further, HHS may elect to impose an additional fine on your firm. And the HIPAA insurance policy your firm carries probably excludes personal devices.

The problem with electronic discovery in so many cases is that, absent proactive measures taken by enterprising lawyers to limit the scope and amount of e-discovery through the many useful strategies CR 26 offers, the amount of ESI collected, processed and ultimately reviewed by attorneys is far too over-inclusive. That mistake and avoiding it is a topic for another day, but this over-inclusiveness increases substantially the risk that irrelevant medical information about a client or client employee can be exposed, and then your firm could be liable as a 'business associate:"

> [H]ealth care providers and other entities traditionally associated with HIPAA … also raise major concerns for the "business associates" of these entities, which often include law firms. In particular, effective Sept. 23, 2013, the Omnibus Rule expanded the accountability of law firm business associates by making them directly responsible for complying with large parts of HIPAA.[3]

Similar pitfalls for negligent disclosure of clients' confidential information are faced by lawyers for schools and school districts in the Federal Educational Rights and Privacy Act (FERPA) and the Child Online Privacy Protection Act (COPPA). There is undoubtedly a whole host of other statutes regulating information exchange and disclosure beyond those mentioned here, where law firms as "business associates" or agents can be drawn into the various circles of liability inferno created by unwanted information leakage.

## Reducing the Risks

So what to do? Here are some practice tips:

*Don't make yourself the expert.* Hire the services of a qualified expert to do a technology and information management audit of any third-party vendor you are contemplating to host your client's data. Make sure that expert follows all the steps outlined in WSBA Opinion 2215. Another option is to elevate or hire a tech-savvy paralegal to serve as the "E-Discovery Liaison" for all e-discovery issues in each of your cases, as that role is defined and contemplated in the interesting three-year e-discovery pilot project initiated by the Seventh Circuit.[4]

This ongoing "experiment" has been an attempt by the bench and bar in the Seventh Circuit to streamline e-discovery. One positive development has been the concept that each litigating party must have available an identified liaison who fully understands the client's computer and information systems and who is responsible for communicating about them intelligently so e-discovery will work better. This requirement can be achieved by local rule change, by court order or by agreement between the parties.

*Work proactively with your clients to get them to isolate sensitive client information so that it is rarely if ever exposed online.* A truly secure computer is one with limited physical access to it and which is never online. Remember, there was a time when no computers were online, and there are many ways to quarantine sensitive data so only those trusted few with a need to know have access.

*Treat data like gold bars.* We use Brinks trucks to move money around. Using the hypothetical from the Tennessee Bar Association publication cited above: The data should not have been put on a thumb drive so it could get easily lost, and it should not have been taken everywhere casually, either. It should have been put in a lockbox with a combination lock and sent by FedEx or UPS directly to its intended destination.

*Do ESI document reviews offline.* Yes, working with certain shared web-based applications can be useful for document reviews, but are they worth the risks? Do you want to read your client's CEO's steamy email in tomorrow's newspaper? Taken from the ESI they entrusted to you?

In large cases, with many reviewers in different geographical locations, the benefits of hosting client data online may be worth the risk. However, for the vast majority of cases, your best choice may be not to host your client data online to reduce vulnerability and risk. ■

---

*Larry G. Johnson is a lawyer in Newcastle, and has been a member of the Washington bar since 1974. He recently served on the E-Discovery Subcommittee of the WSBA Escalating Cost of Civil Litigation (ECCL) Task Force. Besides being a litigator, for the past 20 years he has served as a consultant and expert witness in e-discovery matters. He does business as Electronic Data Evidence (www.e-dataevidence.com).*

[1] *http://mcle.mywsba.org/IO/print.aspx?ID=1662*, issued in 2012. It is worth reading in its entirety.

[2] "PRIVACY: What Lawyers Must Do to Comply with HIPAA, Accountability Expanded for Law Firms Acting as Business Associates," Tennessee Bar Association, March, 2014; *http://www.tba.org/journal/privacy-what-lawyers-must-do-to-comply-with-hipaa*.

[3] *Id.* Footnote omitted.

[4] For more information about this project, see, e.g., *https://apps.americanbar.org/litigation/litigationnews/civil_procedure/docs/barkett.december11.pdf*.