THE ETHICS OF THIRD-PARTY TECHNOLOGY SOLUTIONS

Sarah J. Banola and Joanna L. Storey

It is difficult to choose among the many options for law practice management software available on the market. If your first question is which is the most efficient and reasonably priced, then you have failed to spot the threshold legal issue. Purchasing shiny new software or cloud services without considering your ethical duties may land you in hot water with the State Bar of California, or worse—with your own clients. Here are 10 critical tips for ethically evaluating whether and how to use third-party technology solutions.

1. START AT THE BEGINNING

California Rules of Professional Conduct ("CRPC"), Rule 3-110, governs an attorney's duty to perform legal services with competence and states, in part: "If a member does not have sufficient learning and skill when the legal service is undertaken, the member may nonetheless perform such services competently...by acquiring sufficient learning and skill before performance is required."

You may think this rule applies only to the practice area your matter involves (e.g., a personal injury attorney, taking on a trade secret case without training and skill is ill advised). But the rule applies to more than just your knowledge of the law.[1] As technologies change, security standards may change and an attorney must keep abreast of the current standards to evaluate whether the technology adequately protects the client's confidential information.[2]

2. READ ABA FORMAL OPINION 477

This opinion addressing "Securing Communication of Protected Client Information," presented by the Standing Committee on Ethics and Professional Responsibility of the American Bar Association is a must read for any attorney who transmits client information over the internet. Find it at www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.pdf

3. REMEMBER THE HALLMARK DUTY TO PRESERVE SECRETS

The duty of confidentiality reflects public policy of paramount importance and is not simply a rule of professional conduct.[3] An attorney has a duty to "maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client."[4] Client

[1] See ABA Model Rule 1.1. Cmt. [8] (the duty of competence includes "keeping abreast of...the benefits and risks associated with relevant technology")

[2] Cal. State Bar Formal Opn. 2012-184; see also Cal. State Bar Formal Opn. 2015-193

[3] *In re Jordan*, 7 Cal.3d 930, 940-941 (1972)

"secrets" means information relating to the representation of a client that is privileged, or that the client has asked be kept in confidence, or the disclosure of which would be embarrassing or detrimental to the client.[5] The duty of confidentiality includes, but is not limited to, information that is protected by the attorney-client privilege[6] and the attorney work product doctrine.[7] The duty also prohibits disclosure of a much broader body of information, which can include matters of public record that have been communicated to the attorney in confidence.[8]

Lawyers must take reasonable measures to safeguard confidential client information when using third-party technology services. This includes investigating and monitoring third-party providers, limiting access to confidential information and obtaining written assurances from the provider concerning data security and the handling of security breaches.[9] If a lawyer is not able to evaluate the security of the technology, the lawyer must seek additional information, or consult with someone who possesses the requisite knowledge to ensure compliance with the duties of competence and confidentiality.[10]

4. USE CHECKLISTS

California State Bar Ethics Opinion 2010-179 provides a starting point for evaluating a particular technology.

Consider:

- Security
- The legal ramifications of interception
- The degree of sensitivity of the information
- What may happen if there is inadvertent disclosure
- The urgency of the situation
- The client's instructions and circumstances

For the degree of sensitivity of the information factor, when storing and sharing protected health information, be sure to comply with the privacy, security and omnibus rules outlined in the Health Insurance Portability and Accountability Act and the California Confidentiality of Medical Information Act, if applicable.

California Ethics Opinion 2012-184 provides a framework for considering whether to implement a virtual law office, including evaluating vendor credentials, data security, cloud access across jurisdictional boundaries, the attorney's ability to supervise the vendor, and the client's consent to a paperless office. ABA Formal Opinion 477 (at pages 6-10) also describes reasonable steps lawyers should implement to secure confidential client information.[11] In addition, the New York City Bar provided a checklist for small law firms when using cloud based services, including determining whether the servers are located in jurisdictions with adequate legal protections for data, protecting "against 'end-user' vulnerabilities, such as the failure to use strong passwords or the use of unsecure Internet connections," and promptly notifying clients of a security breach.[12]

5. REVIEW AND NEGOTIATE YOUR TERMS OF SERVICE

Carefully review and negotiate your agreement for cloud services. As an initial step, the cloud provider should be adequately vetted.

Consider:

- Credentials/expertise in the industry
- Security measures utilized/who will have access to the information?
- How the vendor will transmit client information?

---

[4] Business & Professions Code §6068(e)(1)

[5] Cal. State Bar Formal Opns. 1993-133, 1988-96

[6] Cal. Evid. Code §954

[7] Cal. Civ. P. §2018.010 et seq. See CRPC 3-100, Discussion ¶2

[8] See, e.g., *In the Matter of Johnson*, 4 Cal. State Bar Ct. Rptr. 179, 189 (Rev. Dept. 2000)

[9] See Cal. State Bar Formal Opn. 2012-184.

[10] Id.

[11] See also ABA Model Rule 1.6(c), Cmt. [18]

[12] *The Cloud and the Small Law Firm: Business, Ethics and Privilege Considerations*, available at www.nysba.org/workarea/DownloadAsset.aspx?id=66955

- Does the vendor have backup data provisions?
- What measures are in place to prevent lapses in service (e.g. an earthquake), or a prompt return of data if the provider goes out of business or you close your account?
- Should your cloud provider receive a litigation hold notice? Can you require compliance?[13]

In addition, you should ensure that the agreement has sufficient terms relating to data security, such as an agreement by the vendor to:

- Maintain confidential information in strict confidence
- Use confidential information only for your company's benefit
- Comply with all applicable laws, industry standards, and the firm or company privacy policy
- Implement and maintain reasonable security procedures to protect confidential information from unauthorized access

Also consider the extent to which you will be able to supervise the vendor. Auditing by third parties may be limited by cloud providers, but most will conduct their own audits and provide a report. Finally, watch out for indemnity provisions—often the lawyer will have to indemnify the vendor in the event of a security breach.

6. MONITOR SERVICE PROVIDERS AND CONSIDER INSURANCE TO MITIGATE RISKS

Don't rely exclusively on your carefully-negotiated agreement. The duty of competence includes "the duty to supervise the work of subordinate attorney and non-attorney employees or agents."[14] Although attorneys may consult with technology experts to assist them in complying with their duty of competence when using technology, attorneys must adequately supervise their consultants. A qualified paralegal or technology consultant supervised by the attorney should monitor the data being hosted and the security measures to protect it. Audit reports should be requested on a regular basis. As security measures evolve, follow up with the vendor to ensure the vendor complies with current standards. You should also find out whether your professional liability policy covers data breaches and assess whether separate coverage is appropriate.

7. BE MINDFUL OF YOUR DUTY OF COMMUNICATION

The duty of communication requires an attorney to keep the client "reasonably informed about significant developments" and "to promptly respond to reasonable requests for information."[15] Some state bar ethics committees have considered whether cloud computing itself is a significant development that must be communicated to your client. Most opine "no" in light of the ubiquitous use of cloud services by businesses and law firms. Nonetheless, it is important to follow any client instructions relating to the security of the client's information. Technologically sophisticated clients and those in heavily regulated industries, such as banks and hospitals, often establish attorney guidelines or audit measures to protect their data. Beware of security requirements that may be buried in lengthy litigation management guidelines. Even if your client doesn't provide any instructions, you should communicate with your client at the outset of the representation about the use of cloud services and how to appropriately use technology in client communications, particularly when dealing with highly sensitive confidential client information.[16]

[13] See also ABA Formal Opinion 477 at p. 10; Model Rule 5.3, Cmt. [3]

[14] Discussion to CRPC 3-110

[15] CRPC 3-500

[16] See ABA Formal Opn. 477 at p. 11

Depending on the sensitivity of the data and the scope of the representation, some ethics opinions state that client consent may be required.[17]

8. EXERCISE CAUTION WITH WEBSITE BUILDING TOOLS

In addition to the cloud-based services highlighted in the other tips, attorneys should ensure that firm websites comply with current legal requirements. For instance, law firms should consider whether their websites are accessible to individuals with disabilities.

While the Trump administration recently placed anticipated website accessibility guidelines under the Americans with Disabilities Act on the "inactive list" for rulemaking, and courts have issued conflicting opinions on requirements, law firms should still evaluate the costs and benefits of having accessible websites. Law firm websites should also include a privacy notice that describes how the firm collects, uses, and discloses information obtained from visits to the website.[18]

9. MAINTAIN CONTROL OVER TRANSFERRING CLIENT DATA

California Ethics Opinion 2007-174 addresses an attorney's obligation to promptly return the client's file upon request.[19] The file includes electronic communications and other electronically stored data.

Consider whether your law practice management software is capable of transferring client data to a usable form for clients who may not have your proprietary software and also whether metadata from templates that have been copied from other client matters can be scrubbed.

10. BE REASONABLE AND DON'T USE A "ONE SIZE FITS ALL" APPROACH

In addition to technology targeted to law firms, many attorneys question whether it is permissible to use commonly available file hosting services, such as Google Drive or Dropbox. However, the rules and ethical guidelines do not contain any requirements governing the use of a particular technology or security measure. Rather, complying with your ethical obligations requires a fact-specific analysis, including consideration of the factors discussed above, other relevant guidelines, rules, statutes and regulations, and the client's instructions. The standard is one of reasonableness.[20]

Sarah Banola is a partner at Cooper, White & Cooper where she concentrates her practice in the areas of professional responsibility, employment law and regulatory law. She is the immediate past chair of the Bar Association of San Francisco's Legal Ethics Committee. She is also a contributing editor to the professional responsibility chapter of the California Practice Guide on Employment Litigation and the legal malpractice chapter of the California Practice Guide on Claims and Defenses, published by the Rutter Group.

Joanna Storey is an associate at Hinshaw & Culbertson LLP where her litigation practice includes professional liability and product liability. She actively follows privacy, security and ethics developments and is the secretary of The Bar Association of San Francisco's Legal Ethics Committee.

[17] See, e.g., Pennsylvania Bar Ass'n Ethics Opn. 2011-200; New Hampshire State Bar Ass'n Ethics Opn. 2012-13/4

[18] See Cal. Bus. & Prof. Code §§ 22575-22579

[19] See CRPC 3-700(D)

[20] See Cal. State Bar Formal Opn. 2010-179; ABA Formal Opn. 477