ETHICS *Opinions*

By Rules of Professional Conduct Committee

PUBLIC OPINION 19-RPCC-021

PUBLIC Ethics Advisory Opinions

These Public Opinions have been prepared by the Publications Subcommittee of the Louisiana State Bar Association's (LSBA) Rules of Professional Conduct Committee. The issues and topics covered within these opinions originate from actual requests for ethics advisory opinions submitted to the Ethics Advisory Service by lawyer members of the Association.

In selecting topics and issues for publication, the Publications Subcommittee has reviewed opinions referred to it by Ethics Counsel and/or panel members of the Ethics Advisory Service for purposes of determining whether the opinions submitted address issues of interest, importance and/or significance to the general bar and which are not highly fact-sensitive. The Publications Subcommittee has made every effort to promote and maintain confidentiality of the parties involved in the original requests.

Questions, comments or suggestions regarding the opinions, the publication process or the Ethics Advisory Service may be directed to Eric K. Barefield, Professional Programs Ethics Counsel, Louisiana State Bar Association, 601 St. Charles Ave., New Orleans, LA 70130; direct dial (504)619-0122; fax (504)598-6753; email ebarefield@lsba.org.

To review Published Opinions (to date) online, go to: *www.lsba.org/goto/EthicsOpinions*. Click on "Published Opinions."

PUBLIC Opinion 19-RPCC-021[1]

Lawyer's Use of Technology

A lawyer must consider the benefits and risks associated with using technology in representing a client. When a lawyer uses technology in representing a client, the lawyer must use reasonable care to protect client information and to assure that client data is reasonably secure and accessible by the lawyer.[2]

Technology is constantly evolving and changing the practice of law. Lawyers' practices and the tools they use have changed. Consider typewriters versus computers, or regular mail and fax machines as compared to email. Some reasons for a lawyer to consider the benefits of accepting technological changes and adopting different methods to practice law include "saving money, saving time, or improving quality."[3] Technology and the Internet can modify the way a lawyer practices, affecting communication, practice management, handling evidence and data storage. How a lawyer should handle various aspects of technology, including but not limited to email communication with clients or others and the handling of digital or electronic client files or information, has been discussed in ethics opinions and articles around the country.[4]

The consensus is that if a lawyer is going to use technology, that lawyer has a duty to comply with Rules 1.1, 1.3, 1.4, 1.6 and 1.15 of the American Bar Association (ABA) Model Rules of Professional Conduct. Lawyers must use technology competently and diligently. Lawyers have an obligation to protect client information and confidentiality. Lawyers also have an obligation to diligently weigh the use of potential technology considering variables such as risk and a client's individual capacity or availability to use that technology.

This Committee has considered the ethical ramifications stemming from a lawyer's use of technology when practicing law. In its consideration, the Committee believes that the Louisiana Rules of Professional Conduct most likely[5] implicated by a lawyer using technology are Rules 1.1(a),[6] 1.3,[7] 1.4,[8] 1.6[9] 1.15(a)[10] and 5.3.[11]

Competence and Diligence

When a lawyer contemplates the use of technology, that lawyer should remember Rules 1.1 and 1.3 of the Louisiana Rules of Professional Conduct requiring competence and diligence. The lawyer should carefully evaluate whatever technology is being considered and whether client information will be reasonably secure and retrievable by the lawyer. Whether it might be a disaster like a flood or fire or even a breach by a hacker, a lawyer using technology should evaluate risks to a client's files and information, as well as the lawyer's ability to practice without an incapacitating interruption. For instance, does the lawyer have "back-up" systems to retain/recover digital information in the event of a service interruption?

An article in *GPSOLO Magazine* quotes the Director of the FBI in 2012 when he stated at a conference that "I am convinced there are only two types of companies; those that have been hacked and those that will be."[12] As an example, in 2016, a District Attorney's office in Pennsylvania paid ransom to regain access to its computers. The criminals used malware to hold the

DA's office computer network hostage and were later arrested.[13] In 2012, the ABA amended Comment 8 to Rule 1.1 of the ABA Model Rules of Professional Conduct to add language requiring that competence included an expectation that a lawyer should be knowledgeable of both the benefits and risks of the use of technology.[14] While Louisiana does not have comments to its Rules, Rules 1.1(a) and 1.3 are straight-forward even without a specific technological competence/diligence requirement. If a lawyer is not comfortable working with technology, the lawyer should consider the benefits of obtaining advice from another lawyer or consultant knowledgeable about both technology and a lawyer's ethical and professional responsibilities. If relying on a non-lawyer, Rule 5.3 provides: *"With respect to a non-lawyer employed or retained by or associated with a lawyer: . . . (b) a lawyer having direct supervisory authority over the non-lawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer;. . ."* Accordingly, when a lawyer decides to use a non-lawyer technology service provider or computer consultant, that lawyer should take reasonable steps to ensure that ethical standards and responsibilities of the lawyer are met by the conduct of the service provider or consultant. Failure to use technology competently could put a law firm at risk both ethically and financially if the conduct falls below the applicable standard of care.

Communication

Lawyers have a duty to communicate with clients. Rules 1.4(a)(2) and (3) of the Louisiana Rules of Professional Conduct state the communication obligations of a lawyer: *". . . a lawyer shall . . . (2) reasonably consult with the client about the means by which the client's objectives are to be accomplished . . .;"* and *". . . (3) keep the client reasonably informed about the status of the matter; . . . ."* How lawyers choose to communicate with clients is changing, with emails and text messages sometimes replacing phone calls and letters. Lawyers first should be cognizant regarding a potential client's capacity or ability to use technology. In some cases, use of advanced technology with an elderly, underprivileged, unknowledgeable or rural client with limited Internet access might not be reasonable. A lawyer may want to consider the benefit of advising clients regarding potential risks associated with using technology, such as having an inadequate password or other people being aware of their password, as compared to in-person consultations or traditional communication options. When very sensitive information is being communicated, it may be appropriate to consider encryption, as well as to provide the option of communicating by means of more traditional methods. If a lawyer elects to use technology, a lawyer has an obligation to use that technology in a manner that meets all reasonable ethical and professional standards, as well as to advise a client regarding potential risks. Many lawyers use computers to transmit email, pleadings or other documents. Whether using computers at the office or using a mobile device, a lawyer should always consider whether client information is reasonably secure and retrievable by the lawyer. Failure of a lawyer to use basic minimum standards for security, such as secure passwords, firewalls and encryption, may put a lawyer at risk of a potential violation of the Louisiana Rules of Professional Conduct. Strong passwords should be used on all computers and mobile devices, such as smart phones and tablets. When using mobile devices, a lawyer should consider how secure a network might be and whether the option to secure or delete data remotely will be available if the mobile device is misplaced or stolen. If a data breach of material client information were to occur, a lawyer would not only need to take reasonable steps to address the problem, but also to disclose the fact of the breach to the client.[15]

Confidentiality

The modern practice of law is evolving with the use of technology, such as "cloud computing," allowing a lawyer to be more mobile and potentially reducing overhead costs. With Internet access, lawyers can access client data and/or store data practically anywhere. Cloud computing could be defined as using the Internet for the electronic transfer of data and/or storage on a computer or server that is not located in a lawyer's office but in an offsite location. As cited in Pennsylvania's ethics opinion, a *Maximum PC* magazine article described "cloud computing" as "a fancy way of saying stuff is not on your computer."[16] As client information is sent offsite using the "cloud," a lawyer has delegated to others some level of control and security of that data. As a result, the ABA modified its rules in recent years to address technological changes affecting the way lawyers practice. Louisiana, following the ABA's lead on this issue, amended Rule 1.6 of the Louisiana Rules of Professional Conduct in January 2015 specifically to add Part "c": *"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."*[17] Rules 1.6 and 1.15 of the Louisiana Rules of Professional Conduct require a lawyer to protect client confidentiality and client property, stating: *"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). . ."* and *". . .(a) A lawyer shall hold property of clients or third persons that is in a lawyer's possession in connection with a representation separate from the lawyer's own property . . . Other property shall be identified as such and appropriately safeguarded. . . ."*

While there are always risks with the use of technology, a lawyer needs to weigh the benefits of using technology versus any risks that are associated with its use. For example, sending digital files in a non-secure format could allow the inadvertent release of information a lawyer or client would not want shared by the unintentional disclosure

of "metadata," which is information embedded in electronic documents. The ABA issued an ethics opinion regarding those risks in 2006.[18] Additionally, email "web bugs" could track lawyer-client communications. An Alaska ethics opinion has suggested that a lawyer's surreptitious use of email "bugs" or tracking of opposing counsel's email communications with his or her client would be an ethical violation.[19] Irrespective of the wisdom of this conclusion, lawyers must be aware that email "opens" and "forwards" may be tracked and act accordingly. There is always a risk that a lawyer's computer system could be breached. Law firms face the same issues as other companies when it comes to defending against cyber-attacks or hacking and protecting confidential data. Additionally, lawyers have ethical rules that require confidentiality of client information. Thus, if a lawyer chooses to use technology in his/her practice, basic issues must be addressed. The onus is on the lawyer to have technological competence or competent assistance to make sure clients' confidential information or files are reasonably secure and readily accessible, asking questions such as: Are fundamental security measures being met? Are there redundant back-up methods for the storage and retrieval of digital data? Has due diligence research been conducted on prospective service providers?

Supervision, Delegation or Outsourcing

Some lawyers are more comfortable working with and understanding technology than others. While a lawyer cannot relinquish the ultimate responsibility over a client's case, nothing prohibits a lawyer from receiving assistance with technology and related issues from a lawyer's staff or consultants. For example, a lawyer may need assistance regarding eDiscovery or prevention of the spoliation of evidence involving technology. However, if relying on a non-lawyer, Rule 5.3 provides: *"With respect to a non-lawyer employed or retained by or associated with a lawyer: . . . (b) a lawyer having direct supervisory authority over the non-lawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer;. . . ."* Accordingly, when a lawyer decides to use a non-lawyer technology service provider or computer consultant, that lawyer should take reasonable steps to ensure that ethical standards and responsibilities of the lawyer are also met by the conduct of the service provider or consultant.

Issues to Consider When Using a Vendor

Technology continues to evolve, and a lawyer must use due diligence when considering various technological options or providers. For example, when using various technology vendors for things such as a cloud-based practice management system or for data storage, a lawyer must review and consider the service agreement. Some issues and questions a lawyer may want to consider were outlined in an ethics opinion from the Ohio State Bar:[20]

► What safeguards does the vendor have in place to prevent confidentiality breaches?

► Does the agreement create an enforceable obligation on the vendor's part to safeguard the confidentiality of data?

► Do the terms of the agreement purport to give "ownership" of the data to the vendor, or is the data merely subject to the vendor's license?

► How may the vendor respond to governmental or judicial attempts to obtain disclosure of your client data?

► What is the vendor's policy regarding returning your client data at the termination of its relationship with your firm?

► What plans and procedures does the vendor have in case of natural disaster, electronic power interruption or other catastrophic events?

► Where is the server located (particularly if the vendor itself does not actually host the data, and uses a data center located elsewhere)? Is the relationship subject to international law?

The questions listed above are examples for a lawyer to consider when deciding whether to use a particular type of technology, software or service provider. Updated information about various types of technology and a lawyer's practice can be found at the ABA's Legal Technology Resource Center. [21] Additional resources and information about technology can be found on the Louisiana State Bar Association's website.[22]

Conclusion

A lawyer must consider the benefits and risks associated with using technology in representing a client. When a lawyer uses technology in representing a client, the lawyer must use reasonable care to protect client information and to assure that client data is reasonably secure and accessible by the lawyer.

FOOTNOTES

1. The comments and opinions of the Committee — public or private — are not binding on any person or tribunal, including, but not limited to, the Office of Disciplinary Counsel and the Louisiana Attorney Disciplinary Board. Public opinions are those which the Committee has published — specifically designated thereon as "PUBLIC" — and may be cited. Private opinions are those that have not been published by the Committee — specifically designated thereon as "NOT FOR PUBLICATION" — and are intended to be advice for the originally-inquiring lawyer only and are not intended to be made available for public use or for citation. Neither the LSBA, the members of the Committee or its Ethics Counsel assume any legal liability or responsibility for the advice and opinions expressed in this process.

2. In addition to confidentiality issues, a lawyer should consider what happens if a dispute arises with a service provider, what format the data is in, and who owns or retains the rights to the digital data.

3. *Cloud Computing for Criminal Lawyers: It's Not the Future Anymore (2016),* Dane S. Ciolino, Alvin R. Christovich Distinguished Professor of Law, Loyola University New Orleans College of Law.

4. Law Sites, *25 States Have Adopted Ethical Duty of Technology Competence* (March 16, 2015); ABA Formal Opinion 06-442, *Review and Use of Metadata*; Ethics Opinion 2011-200 from Pennsylvania; Ethics Opinion 2012-13/4 from New Hampshire; and Informal Advisory Opinion 2013-03 from Ohio.

5. A myriad of Louisiana Rules of Professional

Conduct could be implicated depending on the facts and situation, such as Rule 7.2, *et. seq.*, involving lawyer advertising or solicitation.

6. Rule 1.1(a) of the Louisiana Rules of Professional Conduct, in pertinent part, provides: *"A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."*

7. Rule 1.3 of the Louisiana Rules of Professional Conduct, in pertinent part, provides: *"A lawyer shall act with reasonable diligence and promptness in representing a client."*

8. Rule 1.4 of the Louisiana Rules of Professional Conduct, in pertinent part, provides: *"Communication. (a) A lawyer shall: . . . (3) keep the client reasonably informed about the status of the matter;. . . (b) The lawyer shall give the client sufficient information to participate intelligently in decisions concerning the objectives of the representation and the means by which they are to be pursued . . . ."*

9. Rule 1.6(a) and (c) of the Louisiana Rules of Professional Conduct, in pertinent part, provides: *". . . (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) . . . (c) 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."*

10. Rule 1.15 of the Louisiana Rules of Professional Conduct, in pertinent part, provides: *". . . (a) A lawyer shall hold property of clients or third persons that is in a lawyer's possession in connection with a representation separate from the lawyer's own property . . . Other property shall be identified as such and appropriately safeguarded . . . ."*

11. Rule 5.3 of the Louisiana Rules of Professional Conduct provides: *". . . With respect to a non-lawyer employed or retained by or associated with a lawyer: (a) a partner, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer; (b) a lawyer having direct supervisory authority over the non-lawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and (c) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if: (1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or (2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action."*

12. "What to Do When Your Data is Breached," *GPSOLO,* Jan./Feb. 2016, Nelson, Ries and Simek.

13. "Prosecutor's Office Paid Ransom to Regain Access to Computers; International Network Busted," *ABA Journal*, 12/6/16.

14. *"[8] 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 a lawyer is subject."*

15. ABA Formal Opinion 18-483, *Lawyers' Obligations After an Electronic Data Breach or Cyberattack.*

16. Quinn Norton, "Byte Rights," *Maximum PC*, September 2010, at 12.

17. This provision was first adopted by the ABA after an Ethics 2020 report which considered changes in the practice due to technology.

18. ABA Formal Opinion 06-442, *Review and Use of Metadata*.

19. Alaska Bar Association Ethics Opinion No. 2016-1.

20. Ohio State Bar Opinion 2013-03, p. 4.

21. *www.americanbar.org/groups/departments_offices/legal_technology_resources.html*.

22. *www.lsba.org/PracticeManagement/TechCenter.aspx*.

LBLS Accepting Requests for Certification Applications

The Louisiana Board of Legal Specialization (LBLS) is accepting applications for certification in the new specialty of health law through March 31, 2019. The LBLS will accept applications for business bankruptcy law and consumer bankruptcy law certification through Sept. 30, 2019.

In accordance with the Plan of Legal Specialization, a Louisiana State Bar Association member in good standing who has been engaged in the practice of law on a full-time basis for a minimum of five years may apply for certification. Further requirements are that, each year, a minimum percentage of the attorney's practice must be devoted to the area of certification sought, and the attorney must pass a written examination to demonstrate sufficient knowledge, skills and proficiency in the area for which certification is sought and provide five favorable references. Peer review is used to determine that an applicant has achieved recognition as having a level of competence indicating proficient performance handling the usual matters in the specialty field. Refer to the LBLS standards for the applicable specialty for a detailed description of the requirements: *www.lsba.org/goto/specialization.*

In addition to the above, applicants must meet a minimum CLE requirement for the year in which application is made and the examination is administered:

► Health Law — 15 hours of approved health law.

► Bankruptcy Law — CLE is regulated by the American Board of Certification, the testing agency.

With regard to applications for business bankruptcy law and consumer bankruptcy law certification, although the written test(s) is administered by the American Board of Certification, attorneys should apply for approval of the LBLS simultaneously with the testing agency to avoid delay of board certification by the LBLS. Information concerning the American Board of Certification will be provided with the application form(s) and can be viewed online at: *www.abcworld.org*.

Anyone interested in applying for certification should contact LBLS Specialization Director Mary Ann Wegmann, email maryann.wegmann@lsba.org, or call (504)619-0128. For more information, go to the LBLS website link listed above.