Formal Ethics Opinion
KENTUCKY BAR ASSOCIATION

Ethics Opinion KBA E-446
Issued: July 20, 2018

The Rules of Professional Conduct are amended periodically. Lawyers should consult the current version of the rule and comments, SCR 3.130 (available at http://www.kybar.org/237), before relying on this opinion.

Subject: Cybersecurity

Question #1: Does an attorney have an ethical responsibility to implement cybersecurity measures to protect clients' information?

Answer: Yes

Question #2: Does an attorney have an ethical responsibility to advise clients about cyberattacks against the law practice and/or breaches of security?

Answer: Qualified Yes.

Question #3: Can an attorney utilize third parties and/or non-lawyers to plan and implement cybersecurity measures?

Answer: Yes.

Question #4: Does an attorney have an ethical responsibility to ensure that law firm employees, as well as third parties employed by, retained by, or associated with the lawyer, comply with the attorney's cybersecurity measures?

Answer: Yes.

INTRODUCTION

An attorney's use of technology in the practice of law has evolved considerably since this Committee first addressed communicating with clients through electronic mail services in 1998.[1] Since that time, Ethics Opinions have discussed the use of domain names,[2] cloud computing,[3] and most recently, communications between attorneys by email.[4] As noted previously, "Technology provides an ever-changing environment in which to apply the Rules of Professional

[1]KBA Ethics Opinion KBA E-403.

[2]KBA Ethics Opinion KBA E-427.

[3]KBA Ethics Opinion KBA E-437.

[4]KBA Ethics Opinion E-442.

Conduct."[5] Whether an attorney uses email to communicate with clients; e-files documents with the courts; stores client information electronically; shares files with others; employs mobile devices and/or accesses the internet, care must be taken to avoid disclosure of confidential client information.

As technology has evolved, so has the ability of third parties to attack or 'hack' a lawyer's electronic systems, not only to obtain confidential client information, but also to disrupt the law firm's operations by threatening to destroy client files to collect ransom payments. "Creating, using, communicating, and storing information in electronic form greatly increases the potential for unauthorized access, use, disclosure and alteration, as well as the risk of loss or destruction (of client information)."[6] Attorneys must therefore be cognizant of cybersecurity measures that can be employed to preserve their client's information.

Unfortunately attorneys are consider 'easy targets' for cyberattacks.[7] If 'techno-challenged', or even 'technophobic', the lawyer may not appreciate the cyber risk of electronically communicating with clients, and/or storing collected client information on the law firm's computer systems. Further, the technology employed by an attorney to protect from unauthorized access, theft, or destruction of client information may not be as sophisticated as the client's own cyber defenses. Moreover, while solo practitioners or small law firms may think they are immune to cyber attacks, the size of a law firm doesn't matter when it comes to cyberattacks. Instead, the 'sophistication or lack thereof' of the attorney's computer system becomes the issue. As learned from the 'Panama Papers' breach, even the largest of law firms whom one would believe would have tech-savy security in place to prevent 'hacks', are not exempt from cyber attacks.[8]

In 2012, the American Bar Association ("ABA") established a "Cybersecurity Legal Task Force" that recommended 'technology amendments' to the Model Rules of Professional Conduct ("Model Rules") 1.0; 1.6; and 4.4. Those amendments were subsequently approved by the ABA House of Delegates to specifically provide information and guidance to attorneys on use of electronic communications; intrusions on a law firm's systems and networks; and ethical obligations to protect a client's confidential information. The ABA Standing Committee on Ethics and Professional Responsibility subsequently issued Formal Opinion 477R on May 22, 2017, that

---

[5] Id.

[6] ABA Cybersecurity Legal Task Force & Section of Science & Technology Law, Report to the House of Delegates: Resolution 109 A.B.A. 4 (August 2014) ("Cybersecurity Resolution").

[7] Jane LeClaire & Gregory Keeley, Cybersecurity in Our Digital Lives (2013) at 128.

[8] "... (T)he Mossack Fonseca (law firm) attack was *dead simple*. So simple, in fact, that a teenager with no hacking knowledge other than basic googling skills could have done it... Furthermore, the security mistakes Mossack Fonesca made were *appallingly common.* So common, in fact, that it's fair to say most of the readers of this article work for organizations that are making at least one of the same mistakes." Jason Bloomberg, "Cybersecurity Lessons Learned from 'Panama Papers' Breach, Forbes Tech Journal (April 21, 2016).

interpreted these amendments to the Model Rules to further explain ethical issues involving the use of electronic means to communicate regarding client matters.[9] While the Kentucky Supreme Court did not adopt the ABA Model Rules, nor has it amended the Kentucky Rules of Professional Conduct ("Rules") [10] to discuss technology issues as the ABA has done, the discussion in Formal Opinion 477R provides a background to an attorney seeking guidance on technology issues impacting confidentiality of client communications.

DISCUSSION

Question 1: An attorney's ethical responsibility to implement cybersecurity measures to protect clients' information is founded upon four (4) separate requirements of the Rules as they relate to competence (SCR 1.1(6)); communications (1.4); confidentiality of information (1.6) and safekeeping of client's property (1.15). Paramount among these ethical obligations is the requirement to "... not reveal information relating to the representation of a client unless the client gives informed consent."[11] The Commission has previously acknowledged that this provision not only applies to traditional paper communications, but it also applies to the use of emails with clients and opposing counsel, as well as the storing of client information 'in the cloud'. Above all, the attorney must use 'reasonable care' to ensure that the client's confidential information is protected, and that the client's property is safeguarded.[12]

Comment (8) to ABA Model Rule 1.1 states that for an attorney to maintain the 'requisite knowledge and skill' required by this provision of the Model Rule, the attorney must keep abreast of the changing risks and benefits of relevant technology[13]. Effective January 1, 2018, the Kentucky Supreme Court similarly revised its "Maintaining Competence" Commentary (6) of SCR 3.130 (1.1) to include "... the benefits and risks associated with relevant technology...." Further, KBA Opinion E-437 makes it clear that Kentucky lawyers should be competent in the use of technology in their law practices. This 'competence requirement' includes the knowledge of

---

[9]For an extensive discussion of this topic, refer to the ABA Cyberscurity Handbook: A Resource for attorneys, law firms, and business professionals (2nd Edition) by Jill D. Rhodes and Robert S. Litt (2018)

[10]SCR 3.130 et seq.

[11]SCR 3.130 (1.6).

[12] See, KBA Ethics Opinion E-437; For a discussion of this Opinion and its practical application to the practice of law, see "Ethics Still Apply: Even When Your Head Is In The Cloud", Lawyers Mutual Insurance Company of Kentucky Risk Management (2016).

[13] The ABA stated that the change to Model Rule 1.1 did not create a 'new requirement' for an attorney, but instead made explicit what was previously considered 'implicit' in the Model Rule; See also, "Andrew Perlman, "The Twenty First Century Lawyer's Evolving Ethical Duty of Competence", The Professional Lawyer, Vol. 22, No. 4.

traditional cyber defense tools to protect client data. Thus, "(b)ecause the protection of confidentiality is an element of competent lawyering, a lawyer should not use any particular mode of technology to store or transmit confidential information before considering how secure it is, and whether reasonable precautions such as firewalls, encryption, or password protection could make it more secure."[14]

It should be noted that the type of communication with a client, and/or the method of storing a client's data may require different levels of security. "At the beginning of the client-lawyer relationship, the lawyer and the client should discuss what levels of security will be necessary for each electronic communication about client matters. Communications to third parties containing protected client information requires analysis to determine what degree of protection is appropriate. In situations where communication (and any attachments) are sensitive or warrant extra security, additional electronic protection may be required."[15]

Due to the constant changing of technology, it is impossible to give specific requirements of what constitutes 'reasonable efforts' by an attorney to prevent cybersecurity breaches.[16] What is 'reasonable' depends upon the facts and circumstances taken to prevent access or disclosure of confidential information. Comment 18 to the Model Rules provides some guidance:

> "Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (eg. By making a device or important piece of software excessively difficult to use)"

By no means, however, is an attorney ethically held to a 'strict liability' standard in efforts to prevent cyber attacks. Nor do we mandate specific measures or suggested safeguards that an attorney must take to avoid 'hacks' in order to satisfy this ethical responsibility.[17] Instead, this Opinion updates historically held ethics guidelines for keeping client information confidential in light of the ever-changing use of technology in the practice of law.

Furthermore, as an attorney is under a continuing obligation pursuant to SCR 3.130

---

[14]California State Bar Opinion 2010-179 (undated).

[15]ABA Formal Opinion 477R at 7.

[16] For a discussion of Data Breach Cyber Security Risk Management see "Attorney's Liability for Data Breaches" Lawyers Mutual Insurance Company of Kentucky Risk Management (2016).

[17]See, Arizona State Bar Opinion 09-04 (2009) which tells attorneys who store client information to consider firewalls, password protection schemes, encryption, certain anti-virus measures, etc.

(1.1) to "... keep abreast of changes in the law and its practice ..."[18] so too is the attorney to undertake continuing technology education to increase cyber-preparedness, and to continually reevaluate policies and procedures in place to minimize data breaches of a client's confidential information.

Question 2: An attorney is required to "... reasonably consult with the client about the **means** by which the client's objectives are to be accomplished."[19] The 'means' employed by the attorney includes discussing the use of technology in client communications, the handling of confidential client information within the law firm, and the storage of that information.[20]

Further, an attorney is required to " . . . keep the client reasonably informed about the status of the matter (that the attorney is handling for the client."[21] The Commentary to this Rule[22] explains that this includes telling the client about 'significant developments' affecting the time or the substance of the representation. While an attorney is allowed to withhold certain information from the client in limited circumstances, "(a) lawyer may not withhold information to serve the lawyer's own interest or convenience or the interests or convenience of another person."[23]

SCR 3.130(1.4) does not mandate the disclosure to a client about general cyber attacks against the law firm, or breaches of security within an attorney's computer systems. However, if there is a disclosure of the client's specific confidential and/or privileged information to third parties, which we believe would constitute a 'significant development' affecting the client's representation, then a disclosure must be made to the client about this development.

We are further mindful of KRS 365.732 which imposes a statutory duty upon an 'information holder'[24] to give written notice to persons affected by a computer security 'breach' involving their unencrypted 'personally identifiable information'. While this statute does not establish a cause of action for a violation, KRS 446.070 allows a person injured by the violation of any Kentucky statute to recover damages sustained as a result of that violation. Thus, if an attorney failed to disclose to the client a breach involving the client's unencrypted personally identifiable information then the attorney may be unethically withholding that information to protect the

---

[18]Supreme Court Commentary (6).

[19]SCR 3.130 (1.4)(a)(2).

[20]See, KBA Opinion E-437 discussing with a client the attorney's use of the cloud if the client's matter is sufficiently sensitive.

[21]SCR 3.130(1.4).

[22]Commentary (3) to SCR 3.130 (1.4).

[23]Commentary (7) to SCR 3.130 (1.4).

[24]KRS 365.732(1) (b) defines an 'information holder' as "... any person or business entity that conducts business in this state."

lawyer's own interest to avoid a lawsuit or an ethical charge by the client.

Similarly, the duty imposed by SCR 3.130 (1.15) to 'safekeep' a client's 'property' not only applies to a trust account in which a client's funds are maintained, but also to the client's files; client data stored on the law firm's computer system or 'the cloud'; and the client's intellectual property retained by the attorney because of pending matters. The Commentary to this Rule explains: "A lawyer should hold property of others with the care required of a professional fiduciary." Accordingly, the theft or loss of a client's funds or property as a result of a cyberattack must also be disclosed to the client.

Question 3: An attorney may not delegate ethical responsibilities to third parties. However, when the attorney lacks sufficient information, education and/or training to comply with the Rules, then the attorney should seek assistance from others, including nonlawyers and/or support services. "Any lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education."[25]

Due to the rapid change of cybersecurity options, an attorney may determine that taking 'reasonable measurers' to avoid a theft or loss of confidential client information includes contracting with a professional to create and/or maintain the cybersecurity plan for the law firm. "When a lawyer selects a provider of any support services, the duty of competence, the duty to protect a client's property, and the duty of confidentiality require the lawyer to investigate the qualifications, competence and diligence of the provider.[26] A lawyer who does not investigate whether a warehouse he or she is considering for the storage of files had adequate security to safeguard client files fails in his or her confidentiality and competence obligations to the client. Likewise, an attorney selecting an online provider of storage or other services must investigate the provider to be sure that client information is reasonably sure to remain confidential and secure."[27]

Notably, each attorney within a law firm does not need to personally have all of the requisite technology competencies to meet this ethical responsibility. The lawyer can utilize another attorney within the law firm, the expertise of the law firm's nonlawyer staff, and/or outside experts to comply. "Getting expert help is a recurring theme (as well as good advice) in ethics opinions on this[28] subject."

Question 4: Partners or managers of attorneys, as well as supervisory lawyers, are required under the Rules to make 'reasonable efforts' to ensure that those lawyers that they manage or supervise

---

[25]ABA Formal Opinion 477R at 9.

[26]For a discussion of what information lawyers should consider in this regard, refer to KBA Opinion E-437 at 6; See also, ABA Formal Opinion 08-451 regarding outsourcing legal and nonlegal services.

[27]Id. at 4-5.

[28]ABA Cybersecurity Handbook, supra at 66.

conform to the Rules.[29] That requirement extends to nonlawyers or assistants employed or retained by, or associated with, a lawyer . Thus, the attorney who has direct supervisory over the nonlawyer must ensure their conduct complies with the Rules.[30]

At the same time, lawyers who have managerial authority within a law firm are required to make " ... reasonable efforts to establish internal policies and procedures designed to provide reasonable assurances that nonlawyers in the firm will act in a way compatible with the Rules...." [31] While all lawyers have a duty to evaluate their client data and systems and take reasonable steps to secure confidential information, attorneys who have managerial roles have the added duty of evaluating and correcting security issues within the law firm and prescribing policies and procedures to reduce cyber threats. Having an effective data security program will reduce the risk of confidential client information being disclosed for all lawyers in the law firm.

The Opinion does not mandate the specific policies or procedures that an attorney must employ to have an effective data security program, nor does it contend that there is a 'one shoe fits all' solution for every attorney for cybersecurity. Instead, each attorney must understand what devices the law firm uses that are connected to the office network or the internet; how client information is exchanged or stored through that system and who has access to the data, and make 'reasonable efforts' to combat cyber threats. An attorney's policies will thus depend upon an attorney's use of electronics; the method used to communicate with clients and the nature of the client's information.[32] "These requirements are as applicable to electronic practices as they are to comparable office procedures."[33]

Establishing policies and procedures for cybersecurity alone, however, does not end the partner, attorney manager or supervising attorney's responsibility under the Rules. Implementation of the policies and procedures, specific training for employees on those policies and ongoing supervision is warranted. Because a law firm's data security practices are only as strong as its weakest link " (all lawyers) must make sure that subordinate attorneys, interns, paralegals, case managers, administrative assistants, and external business partners all understand necessary data security practices and the critical role that all parties play in ensuring the protection of client information."[34]

---

[29]SCR 3.130 (5.1).

[30]SCR 3.130 (5.3).

[31]Commentary (2) to SCR 3.130 (5.3); See also Commentary (2) to SCR 3.130 (5.1).

[32]For a thorough discussion of this topic, refer to the Cybersecurity For The Home and Office: The Lawyer's Guide to Taking Charge of Your Own Information Security by John Bandler (American Bar Association Section of Science & Technology, 2017).

[33]ABA Formal Opinion 477R at 9.

[34]Drew T. Simshaw, "Legal Ethics and Data Security: Our Individual and Collective Obligation to Protect Client Data", 38 Am. J. Trial Advocacy, 549, 550, 554 (2015).

Note To Reader

This ethics opinion has been formally adopted by the Board of Governors of the Kentucky Bar Association under the provisions of Kentucky Supreme Court Rule 3.530. This Rule provides that formal opinions are advisory only.