141

Ethical Duties Arising from Data Breach

Adopted July 20, 2020

Issue

What ethical obligations arise from a breach of a lawyer's data systems?

Introduction

In July 2018, the Colorado Bar Association Ethics Committee (Committee) updated CBA Formal Op. 90, "Preservation of Client Confidences in View of Modern Communications Technology" (2018). The Committee originally published Formal Op. 90 in 1992, long before the advent of smartphones and widespread use of e-mail. Revised Opinion 90 advises that, because technology is constantly evolving, a lawyer's manner of preserving client confidences must be shaped by a competent understanding of the technology used by the lawyer and client to communicate. The Committee's approach is supported by ABA Comm. on Ethics and Prof. Resp., Formal Op. 477R, "Securing Communication of Protected Client Information" (2017) (hereinafter ABA Formal Op. 477R).

In October 2018, the ABA Standing Committee issued ABA Comm. on Ethics and Prof. Resp., Formal Op. 483, "Lawyers' Obligations After an Electronic Data Breach or Cyberattack" (2018) (hereinafter ABA Formal Op. 483). Intended to "pick[] up where

Opinion 477R left off, [Opinion 483] discusses an attorney's ethical obligations when a data breach exposes client confidential information." *Id.*

The Committee concurs with ABA Formal Op. 483's guidance. It similarly uses revised CBA Formal Op. 90 regarding preservation of client confidences as a jumping off point. This opinion does not address state or federal statutory notification obligations that may exist separate from a lawyer's ethical obligations, nor does it address obligations that may be owed to third parties.[1]

Syllabus

A lawyer must make reasonable efforts to prevent, monitor for, halt, and investigate any security breach of data the lawyer controls. In the event of a breach, a lawyer timely must notify current clients and affected third persons.

Discussion

A lawyer must make reasonable efforts to prevent, monitor for, halt, and investigate any security breach[2] involving data that the lawyer controls.[3] What is reasonable depends upon the circumstances. Given the fluid nature of technological advance and the means of exploitation, what is reasonable will evolve over time. *See*

[1] *See*, *e.g.*, C.R.S. §§ 6-1-713.5 – 6-1-716. Colorado lawyers should be aware of statutory notification obligations.

[2] The ABA Standing Committee defines a "data breach" for purposes of ABA Formal Op. 483 as "a data event where material client confidential information is misappropriated, destroyed, or otherwise compromised, or where a lawyer's ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode." ABA Formal Op. 483, p. 4. The Committee adopts those terms for purposes here.

[3] Control is an issue of fact. A lawyer controls the data stored on his electronic infrastructure. A separate issue is control in the use of third-party non-lawyer vendors. *See* ABA Formal Op. 477R, pp. 9-10.

Colo. RPC 1.1, cmt. [8] ("To maintain the requisite knowledge and skill, a lawyer should keep abreast of … changes in … technologies."). Because data security and data breaches frequently present complex, daunting issues outside of a lawyer's expertise, "[a] lawyer's competency in this regard may be satisfied either through the lawyer's own study or investigation or by employing or retaining qualified lawyer and nonlawyer assistants." ABA Formal Op. 483, p. 4; *see also* Colo. RPC 5.3, cmt. [3] ("When using such services outside the firm, a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations. The extent of this obligation will depend upon the circumstances, including the education, experience and reputation of the nonlawyer; the nature of the services involved; the terms of any arrangements concerning the protection of client information; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality.").

Colo. RPC 1.6(c) requires "[a] lawyer [to] make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Comment [18] to Rule 1.6 identifies several factors to consider in determining if this duty is met:

> *Reasonable Measures to Preserve Confidentiality*
>
> [18] Paragraph (c) requires a lawyer to make reasonable efforts to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

> **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 (e.g., by making a device or important piece of software excessively difficult to use)** …

Id. (emphasis added).

Colo. RPC 5.1 and 5.3 obligate a lawyer reasonably to assure that other lawyers, office staff, and outside vendors conform their work to the Rules of Professional Conduct (Rules). Thus, a lawyer has an ethical duty to employ reasonable efforts to monitor law office resources that are connected to the Internet or external data sources and vendors providing related services. *See* ABA Formal Op. 483, p. 5. However, “an ethical violation does not necessarily occur if a cyber-intrusion or loss of electronic information is not immediately detected.” *Id.* Similarly, a lawyer’s “competence in preserving a client’s confidentiality is not a strict liability standard and does not require the lawyer to be invulnerable or impenetrable. Rather, the obligation is one of reasonable efforts to prevent the loss or access.” *Id.,* p. 9.

A data breach may take one of three forms, namely, an intrusion that: (1) results in the misappropriation of electronically-stored information (ESI); (2) destroys or alters ESI; or (3) causes ESI to become temporarily or permanently inaccessible, such as with a crypto-locking attack. A lawyer has an obligation to act reasonably and promptly to stop a data breach once discovered and to attempt to mitigate any damage. *See* ABA Formal Op. 483, p. 6 (citing Rule 1.1). Colorado lawyers should develop an incident response plan of reasonable scope in advance of any breach to meet that obligation.

See Jill D. Rhodes & Roberts S. Litt, *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals* (2d ed. 2018), p. 202.

"When a data breach occurs involving, or having a substantial likelihood of involving, material client confidential information a lawyer has a duty to notify the client of the breach." ABA Formal Op. 483, p. 11. Notice is required in order to "keep the client reasonably informed about the status of the matter," and should explain the intrusion "to the extent reasonably necessary to permit the client to make informed decisions regarding the representation." Colo. RPC 1.4(a)(3) and (b). For an event rendering electronically-stored information inaccessible, a client must be notified if the lawyer's provision of services for which she was hired are significantly impaired by the intrusion. *See* ABA Formal Op. 483, p. 4.

In both instances, a lawyer must make reasonable efforts to determine what occurred during the breach and make "all reasonable efforts to restore computer operations." *Id.*, p. 7. Colorado lawyers should implement a data backup plan that will permit restoration of data without substantially impacting the lawyer's ongoing performance. Any losses should be borne by the lawyer as an overhead expense.

Due to a lawyer's client file retention obligations arising out of Colo. RPC 1.16A, a significant amount of the data in a lawyer's custodial control may relate to former clients. Colo. RPC 1.9(c)(2) directs that "[a] lawyer who has formerly represented a client in a matter … shall not thereafter … reveal information relating to the representation except as these Rules would permit or require with respect to a client." *Id*. Because Rule 1.9 "does not describe what steps, if any, a lawyer should take if such information is revealed," the ABA Standing Committee was "unwilling to require notice to a former client as a matter of legal ethics in the absence of a black letter provision requiring such notice." ABA Formal Op. 483, p. 13.

The Committee is similarly unwilling. However, "as a matter of best practices, lawyers are encouraged to reach agreement with clients before conclusion, or at the termination, of the relationship about how to handle the client's electronic information that is in the lawyer's possession." ABA Formal Op. 483, p.12; *see also* Colo. RPC 1.16(d) (duty to surrender papers to which the client is entitled upon termination of representation); 1.16A (client file retention).