HWG

The Ethics of Cybersecurity

Deepika H. Ravi & Hilary P. Gerzhoy

HWG LLP

HWG

Introduction

HWG

Agenda

1. Competence: Technological Know-How
2. Competence Case Studies: Social Media, E-Discovery, and Metadata
3. Confidentiality: The Rule and the Reasonability Standard
4. Storing Data in the Cloud: Where Competence and Confidentiality Meet
5. Communication: When and How Do You Communicate a Data Breach?
6. Supervision: How Do You Supervise Trained Professionals?

HWG

Competence: Technological Know-How

HWG

VA Rule 1.1

"A lawyer shall provide competent representation to a client. Competent representation requires the **legal knowledge, skill, thoroughness and preparation** reasonably necessary for the representation."

– Va. Rules of Pro. Conduct r. 1.1 (emphasis added)

HWG

VA Rule 1.1

"To maintain the requisite knowledge and skill, a lawyer should engage in continuing study and education in the areas of practice in which the lawyer is engaged. **Attention should be paid to the benefits and risks associated with relevant technology**."

– Va. Rules of Pro. Conduct r. 1.1 cmt. [6] (emphasis added)

HWG

ABA Rule 1.1, Cmt. 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 the lawyer is subject."

– ABA Model Rules of Pro. Conduct r. 1.1 cmt. [8] (emphasis added)

D.C. Ethics Op. 371

"Because of society's embrace of technology, a lawyer's ignorance or disregard of it . . . presents a risk of ethical misconduct."

– D.C. Bar Legal Ethics Comm., Ethics Op. 371 (2016)

Other Jurisdictions' Rule 1.1 Analysis

"This general principle requires lawyers to have a basic understanding of the risks posed when using a given technology and, if necessary, **obtain help from appropriate technology experts** on assessing those risks and taking reasonable steps to prevent data breaches which potentially can harm clients. The threshold obligation to understand the risks is satisfied by learning where and how confidential information is **vulnerable to unauthorized access**. This inquiry must be made with respect to each type of electronic device or system as they have been or are incorporated into the lawyer's practice."

– Cal. State Bar Comm. on Pro. Resp. and Conduct,
Formal Op. No. 2020-203 (2020) (emphasis added)

How to Become Competent

As with all aspects of a lawyer's representation, if a lawyer lacks the requisite competence, he has three options:

"(1) acquire sufficient learning and skill before performance is required;
(2) associate with or consult technical consultants or competent counsel; or
(3) decline the client representation."

Jill D. Rhodes & Robert S. Litt, ABA Cybersecurity Handbook at ch. 6, § II(B) (ABA Publishing ed., 2d ed. 2017) (quoting Cal. State Bar Comm. on Pro. Resp. and Conduct, Formal Op. 2015-193 (2015)).

HWG

How to Become Competent

See also D.C. Rules of Pro. Conduct r. 1.1 cmt. [2] (emphasis added) ("Competent representation can also be provided **through the association of a lawyer of established competence in the field in question**.").

HWG

Competence By Hiring Professionals

A lawyer can satisfy his duty of competence with regards to technological know-how by, for example, **hiring a qualified staff person**.

- *See* ABA Comm. on Ethics & Pro. Resp., Formal Op. 483 (2018) (emphasis added) ("[A] competent lawyer must use and maintain those technologies in a manner that will reasonably safeguard property and information that has been entrusted to the lawyer. A lawyer's competency in this regard may be satisfied either through the lawyer's own study and investigation **or by employing or retaining qualified lawyer and nonlawyer assistants**.").

Competence Case Studies

Competence: Social Media

D.C. Bar Legal Ethics Comm., Ethics Op. 371 (2016): Social Media

- May require searching client's social media for relevant evidence
- Subject to review by adversaries
- Inclusion in discovery requests and responses
- No ex parte contact with decision-makers
- No communication (e.g., a "friend" request) with represented party
- Communicating with clients over social media typically not advisable or appropriate
- Avoid spoilation allegations

HWG

Competence: E-Discovery

Federal Rule of Civil Procedure 26(b)(1)

- Parties may obtain discovery about a relevant matter that is proportional to the needs of the case.
- Factors to consider include:
  1. The parties' relative access to relevant information
  1. The parties' resources
  2. Importance of discovery in resolving issues
  3. Weigh burden/expense v. benefit
- Requires competence in:
  - Scope of e-discovery
  - Review of e-discovery

HWG

Competence: Metadata

What is it?

- Data about data
- Typically not visible from face of the document, but retrievable
- Examples:
  1. Document author
  2. Date document created
  3. Last modified
  4. Last opened

Competence: Metadata

Can lead to

- Inadvertent disclosure of work product
- Inadvertent spoilation

Work product metadata	Evidentiary metadata
Client confidence	Not a client confidence
Must strip before a document is disclosed	Must retain and possibly produce

Competence: Metadata

"A lawyer who receives a document or electronically stored information relating to the representation of the lawyer's client and **knows or reasonably should know** that the document or electronically stored information is privileged and was inadvertently sent shall **immediately terminate review** or use of the document or electronically stored information, **promptly notify** the sender, and **abide by** the sender's instructions to return or destroy the document or electronically stored information."

– Va. Rules of Pro. Conduct r. 4.4(b) (emphasis added)

Competence: Metadata

"For purposes of this Rule, 'document or electronically stored information' includes, in addition to paper documents, email and other forms of electronically stored information, including embedded data (commonly referred to as '**metadata**'), **that is subject to being read or put into readable form**. Metadata in electronic documents creates an obligation under this Rule only if the receiving **lawyer knows or reasonably should know that the metadata was inadvertently sent to the receiving lawyer and that it contains privileged information**."

– Va. Rules of Pro. Conduct r. 4.4 cmt. [2] (emphasis added)

Confidentiality: The Rule and the Reasonability Standard

HWG

VA Rule 1.6

"A lawyer shall not reveal information protected by the attorney-client privilege under applicable law or other information gained in the professional relationship that **the client has requested be held inviolate or the disclosure of which would be embarrassing or would be likely to be detrimental to the client** unless the client consents after consultation, except for disclosures that are impliedly authorized in order to carry out the representation, and except as stated in paragraphs (b) and (c)."

– Va. Rules of Pro. Conduct r. 1.6(a) (emphasis added)

VA Rule 1.6

"A lawyer **shall make reasonable efforts** to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information protected under this Rule."

– Va. Rules of Pro. Conduct r. 1.6(d) (emphasis added)

HWG

VA Rule 1.6

"Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to:

1. the **sensitivity** of the information
2. the **likelihood of disclosure** if additional safeguards are not employed
3. the employment or engagement of persons **competent with technology**
4. the **cost** of employing additional safeguards
5. the **difficulty** of implementing the safeguards, and
6. 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**)."

– Va. Rules of Pro. Conduct r. 1.6 cmt. [19] (emphasis added)

VA Rule 1.6

"To comply with this Rule, a lawyer **does not need to have all the required technology competencies**. The lawyer can and more likely must turn to the **expertise of staff or an outside technology professional**. Because threats and technology both change, lawyers should periodically review both and enhance their security as needed; steps that are reasonable measures when adopted may become outdated as well."

– Va. Rules of Pro. Conduct r. 1.6 cmt. [20] (emphasis added)

VA Rule 1.6

"Because of evolving technology, and associated evolving risks, law firms **should keep abreast on an ongoing basis** of reasonable methods for protecting client confidential information, addressing such practices as . . ."

– Va. Rules of Pro. Conduct r. 1.6 cmt. [21] (emphasis added)

VA Rule 1.6

a. "Periodic **staff security training** and evaluation programs, including precautions and procedures regarding data security;
b. Policies to address **departing employee's** future access to confidential firm data and return of electronically stored confidential data;
c. Procedures addressing **security measures for access of third parties** to stored information . . ."

– Va. Rules of Pro. Conduct r. 1.6 cmt. [21] (emphasis added)

HWG

VA Rule 1.6

d. “Procedures for both the backup and storage of firm data and steps to securely **erase or wipe electronic data** from computing devices before they are transferred, sold, or reused;

e. The use of **strong passwords** or other authentication measures to log on to their network, and the security of password and authentication measures; and

f. The use of **hardware and/or software measures** to prevent, detect and respond to malicious software and activity.”

– Va. Rules of Pro. Conduct r. 1.6 cmt. [21] (emphasis added)

HWG

Reasonable Efforts

- "'Reasonable' or 'reasonably' when used in relation to conduct by a lawyer denotes the **conduct of a reasonably prudent and competent lawyer**." ABA Model Rules of Pro. Conduct r. 1.0(h) (emphasis added).

- *See also* Shea Boyd, The Attorney's Ethical Obligations with Regard to the Technologies Employed in the Practice of Law, 29 Geo. J. Legal Ethics 849, 851-52 (2016) (emphasis added) ("In assessing whether reasonable efforts were made [in accordance with Rule 1.6] the Model Rules suggest essentially a cost/benefit analysis, **weighing the sensitivity of the information and the costs of employing additional safeguards**.").

HWG

Reasonable Efforts

- Other jurisdictions require "reasonable" measures to protect client info.
- *See* Ala. State Bar Off. of Gen. Couns., Ethics Op. 2010-02 (2010) (emphasis added) ("The lawyer must have reasonable measures in place to protect the integrity and **security of the electronic file**. . . . The lawyer should also take reasonable steps to ensure that the files are **secure from outside intrusion**. Such steps may include the installation of firewalls and intrusion detection software.").
- N.J. Advisory Comm. on Pro. Ethics, Op. 701 (2006) (emphasis added) (analyzing Rule 1.6 and holding that a lawyer "is required to exercise sound professional judgment on the steps necessary to secure client confidences **against foreseeable attempts at unauthorized access**").

HWG

ABA Formal Op. 477R

"**Law firms are targets for two general reasons**:

(1) they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client, and

(2) the information in their possession is more likely to be of interest to a hacker and likely less voluminous than that held by the client."

– ABA Comm. on Ethics & Pro. Resp., Formal Op. 477R at 2 (2017) (emphasis added)

HWG

ABA Formal Op. 477R

Case-by-case analysis: "What **constitutes reasonable** efforts is not susceptible to a hard and fast rule, but rather **is contingent upon a set of factors**. In turn, those factors depend on the multitude of possible types of information being communicated (ranging along a spectrum from highly sensitive information to insignificant), the methods of electronic communications employed, and the types of available security measures for each method."

– ABA Comm. on Ethics & Pro. Resp., Formal Op. 477R at 4 (2017) (emphasis added)

HWG

Reasonable Efforts

- What if there is a data breach?
- The Rules **do not impose a strict liability standard**.
- *See* ABA Comm. on Ethics & Pro. Resp., Formal Op. 483 at 9 (2018) (emphasis added) ("[A]n attorney'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**. Rule 1.6 is not violated even if data is lost or accessed if the lawyer has made reasonable efforts to prevent the loss or access.").

Reasonable Efforts

"Paragraph (d) requires a lawyer to act reasonably to safeguard information protected under this Rule 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. . . . **The unauthorized access to, or the inadvertent or unauthorized disclosure of, confidential information does not constitute a violation of this Rule if the lawyer has made reasonable efforts to prevent the access or disclosure**."

– Va. Rules of Pro. Conduct r. 1.6 cmt. [19] (emphasis added)

HWG

Reasonable Efforts

"[A] lawyer is not subject to discipline under this Rule if the lawyer has made reasonable efforts to protect electronic data, even if **there is a data breach, cyber-attack or other incident resulting in the loss, destruction, misdelivery or theft of confidential client information**. Perfect online security and data protection is not attainable. Even large businesses and government organizations with sophisticated data security systems have suffered data breaches."

– Va. Rules of Pro. Conduct r. 1.6 cmt. [20] (emphasis added)

Reasonable Efforts

"Nevertheless, **security and data breaches have become so prevalent that some security measures must be reasonably expected** of all businesses, including lawyers and law firms. Lawyers have an ethical obligation to implement reasonable information security practices to protect the confidentiality of client data."

– Va. Rules of Pro. Conduct r. 1.6 cmt. [20] (emphasis added)

HWG

Reasonable Efforts

- Whether a lawyer took "reasonable" precautions consistent with his Rule 1.6 obligations **is not measured by whether a cyberattack occurred**.
- *See* Jill D. Rhodes & Robert S. Litt, ABA Cybersecurity Handbook at ch. 6, § II(A)(3) (ABA Publishing ed., 2d ed. 2017) ("[I]t is important to bear in mind that, under the rules of professional conduct, the security measures that lawyers are required to put in place are not required to be invulnerable.").
- Conn. Bar Ass'n Pro. Ethics Comm., Informal Op. 2013-07 (2013) ("The duty of confidentiality described in Rule 1.6 is rigid but tempered by the recognition that even when a lawyer acts competently to preserve the confidentiality of the data, reasonable safeguards sometimes fail . . . .").

Reasonable Efforts: An Evolving Standard

"Lawyers have a reasonable expectation of privacy in communications made by all forms of e-mail, including unencrypted e-mail sent on the Internet, despite some risk of interception and disclosure. It therefore follows that its use is consistent with the duty under Rule 1.6 to use reasonable means to maintain the confidentiality of information relating to a client's representation."

– ABA Comm. on Ethics & Pro. Resp., Formal Op. 99-413 (1999)

HWG

Reasonable Efforts: An Evolving Standard

"[T]he use of unencrypted routine email generally remains an acceptable method of lawyer-client communication. However, cyber-threats and the proliferation of electronic communications devices have changed the landscape and it is not always reasonable to rely on the use of unencrypted email. . . . Therefore, **lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters** . . . ."

– ABA Comm. on Ethics & Pro. Resp., Formal Op. 477R at 5 (2017) (emphasis added)

HWG

Storing Data in the Cloud: Where Competence and Confidentiality Meet

HWG

The Cloud

What is the cloud?

The Cloud

"SaaS and Cloud Computing refer to a constellation of web-based data processing, transmission, and storage services that are available over the internet."

– Vt. Bar Ass'n Pro. Resp. Comm., Advisory Ethics Op. 2010-6 at 2 (2010)

"[M]erely 'a fancy way of saying **stuff not on your [own] computer**.'"

– Pa. Bar Ass'n Comm. on Legal Ethics & Pro. Resp.,
Formal Op. 2011-200 at 1 (2011) (emphasis added)

HWG

The Cloud

"[Software as a service] is distinguished from traditional software in several ways. Rather than installing the software to your computer or the firm's server, SaaS is accessed via a web browser (like Internet Explorer or FireFox) over the Internet. . . . SaaS involves storing client information on computer servers that are not owned and operated by the lawyer or law firm . . . ."

– Iowa State Bar Comm. on Ethics & Practice Guidelines,
Ethics Op. 11-01 at 1 (2011)

HWG

The Cloud

"SaaS for law firms may involve the storage of a law firm's data, including client files, billing information, and work product, on remote servers rather than on the law firm's own computer and, therefore, outside the direct control of the firm's lawyers."

– N.C. State Bar Council, Formal Ethics Op. 2011-6 (2012)

- Online billing platform
- Gmail
- Westlaw
- Square
- Online fax services
- Dropbox
- Evernote

The Cloud

Is storing information in the cloud consistent with the ethics rules?

The Cloud

Yes, so long as reasonable precautions are taken.

HWG

The Cloud

"When a lawyer is using cloud computing or any other technology that involves the use of a third party for the storage or transmission of data, the lawyer must follow **Rule 1.6(b)(6) and exercise care in the selection of the vendor**, have a reasonable expectation that the vendor will **keep the data confidential** and inaccessible by others, and **instruct** the vendor to preserve the confidentiality of the information. The lawyer will have to examine the third party provider's use of technology and terms of service in order to know whether it adequately safeguards client information, and if the lawyer is not able to make this assessment on her own, she will have to consult with someone qualified to make that determination."

– Va. State Bar Comm. on Legal Ethics, Legal Ethics Op. 1872 at 3 (2019) (emphasis added)

HWG

The Cloud

"The lawyer is not required, of course, to absolutely guarantee that a breach of confidentiality cannot occur when using an outside service provider. Rule 1.6 only requires the lawyer to act with reasonable care to protect information relating to the representation of a client."

– Va. State Bar Comm. on Legal Ethics, Legal Ethics Op. 1872 at 3 (2019)

HWG

The Cloud

- *See, e.g.*, Neb. State Bar Ass'n Ethics Advisory Comm., Op. 19-01 at 1 (2019) (emphasis added) ("An attorney may transmit information relating to the representation of a client over the internet and allow for that information to be stored on, and accessed through, third-party, off-site servers (generically referred to as 'the Cloud'), if the lawyer has undertaken reasonable efforts to: (1) **prevent inadvertent or unauthorized** access to that information; (2) **maintain the confidentiality of the information**; and (3) **establish reasonable safeguards** to ensure the information is protected from loss, breaches, business interruptions, and other risks created by advancements in technology.").

The Cloud

- Alaska State Bar Off. of Gen. Couns., Ethics Op. 2014-3 at 1 (2014) ("With the issuance of this opinion, Alaska joins the community of bar associations concluding that cloud computing is permissible so long as reasonable steps to protect the client are taken.").

HWG

The Cloud: What Constitutes Reasonable Care?

- The New Jersey Advisory Committee on Professional Ethics opined in analyzing New Jersey's Rule 1.6(f), "[t]he touchstone in using 'reasonable care' against unauthorized disclosure is that:
  - (1) the lawyer has entrusted such documents to an outside provider under circumstances in which there is an **enforceable obligation to preserve confidentiality and security**, and
  - (2) use is made of available technology to guard against **reasonably foreseeable attempts to infiltrate the data**.
- If the lawyer has come to the prudent professional judgment he has satisfied both these criteria, then 'reasonable care' will have been exercised."

– N.J. Advisory Comm. on Pro. Ethics, Op. 701 (2006) (emphasis added)

HWG

The Bottom Line

1. Protect confidentiality and availability of client information via contract and security settings
2. Ban secondary access and use
3. Regularly reassess appropriateness of cloud provider security
4. Have backups and disaster recovery plan
5. Check if your jurisdiction has specific recommendations or requirements

HWG

Clients Can Request Additional Measures

- *See* Jill D. Rhodes & Robert S. Litt, ABA Cybersecurity Handbook at ch. 6, § II(A) (ABA Publishing ed., 2d ed. 2017) (emphasis added) ("**A client may require the lawyer to implement special security measures not required by this Rule**.").

- A lawyer needs to follow her client's reasonable requests.

HWG

Communication: When and How Do You Communicate a Data Breach?

HWG

VA Rule 1.4

"(a) A lawyer shall keep a **client reasonably informed about the status of a matter** and promptly comply with reasonable requests for information.

(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

(c) A lawyer shall inform the client of facts pertinent to the matter and of communications from another party that may significantly affect settlement or resolution of the matter."

– Va. Rules of Pro. Conduct r. 1.4 (emphasis added)

HWG

Rule 1.4: How Often Do You Need to Communicate?

- The "'guiding principle' for evaluating conduct under Rule 1.4 is whether the lawyer fulfilled '**reasonable client expectations for information**' consistent with the lawyer's 'duty to act in the client's best interests' and the client's overall objectives." *In re Ekekwe-Kauffman*, 210 A.3d 775, 789 (D.C. 2019) (quoting D.C. Rules of Pro. Conduct r. 1.4 cmt. [3]) (emphasis added).

- However, "[a]n attorney need not communicate with a client as often as the client would like, as long as the attorney's conduct was reasonable under the circumstances." *In re Schoeneman*, 777 A.2d 259, 264 (D.C. 2001).

HWG

Rule 1.4: What Do You Need to Communicate?

- If you think your client's information may have been stolen in a cyber attack, what do you do?
- It may take time to understand the scope of a breach.
- ABA Comm. on Ethics & Pro. Resp., Formal Op. 483 at 7-8 (2018) (emphasis added) ("The information gathered in a **post-breach investigation** is necessary to understand the scope of the intrusion and to allow for **accurate disclosure** to the client consistent with the lawyer's duty of communication and honesty under Model Rules 1.4 and 8.4(c).").

Rule 1.4: How Quickly Do You Need to Communicate?

- Mich. State Bar Pro. Ethics Comm., Ethics Op. RI-381 (2020) (emphasis added) ("A lawyer has a duty to **inform a client of a material data breach in a timely manner**. . . . A data breach is 'material' if it involves the unauthorized access, destruction, corruption, or ransoming of client ESI protected by [Michigan Rule of Professional Conduct] 1.6 or other applicable law, or materially impairs the lawyer's ability to perform the legal services for which the lawyer has been hired.").

Supervision: How Do You Supervise Trained Professionals?

VA Rule 5.3: Supervision

"[A] partner or a lawyer who individually or together with other lawyers possesses 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** . . . ."

– Va. Rules of Pro. Conduct r. 5.3(a) (emphasis added)

VA Rule 5.3: Supervision

"[A] lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer . . . ."

– Va. Rules of Pro. Conduct r. 5.3(b)

HWG

VA Rule 5.3: Supervision

"[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 managerial authority** in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows or should have known of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action."

– Va. Rules of Pro. Conduct r. 5.3(c) (emphasis added)

HWG

Rule 5.3: Supervision

The duty to supervise nonlawyer staff pursuant to Rule 5.3 is the duty to "have in place **reasonable measures** to ensure that lawyer and nonlawyer personnel are reasonably competent for their intended responsibilities and thereafter receive appropriate training, supervision, and support allowing them to recognize and carry out their responsibilities."

– Restatement (Third) of the Law Governing Lawyers § 11 cmt. g (2000) (emphasis added)

HWG

Rule 5.3: Supervision

"[A] lawyer should be able to verify a prospective translator's or interpreter's professional qualifications in the same manner used when engaging the services of an expert, **i.e., by evaluating the individual's training, experience, certifications, and professional standing**."

– ABA Comm. on Ethics & Pro. Resp., Formal Op. 500 at 7 n.28 (2021) (emphasis added)

Rule 5.3: Supervision What's Required?

See Eli Wald, Legal Ethics' Next Frontier: Lawyers and Cybersecurity, 19 Chap. L. Rev. 501, 525 (2016) (emphasis added) ("It is also worth noting the limits of a lawyer's duties under the rules . . . [**a lawyer need] not to become an expert in information technology**.").

HWG

Rule 5.3: Supervision What's Required?

- Wash. State Bar Ass'n Comm. on Pro. Ethics, Advisory Op. 2215 (2012) (emphasis added) ("It is also impractical to expect every lawyer who uses such services to be able to understand the technology . . . **A lawyer using such a service must, however, conduct a due diligence investigation of the provider** . . . .").
- Cal. State Bar Comm. on Pro. Resp. & Conduct, Formal Op. 2010-179 at 5 (2010) (emphasis added) (an attorney need not "develop a mastery of the security features and deficiencies of each technology available" but advising that if an attorney lacks the expertise to evaluate cloud providers, "he or she **must seek additional information or consult with someone who possesses the necessary knowledge, such as an information technology consultant**").

HWG

Final Thoughts

"[T]he profusion of digital technologies has added cybersecurity to every client's primary interests, whether or not the client knows it, **thereby drawing cybersecurity into the field of view that counsel must watch over if it is to provide competent representation of a client.**"

– Jill D. Rhodes & Robert S. Litt, ABA Cybersecurity Handbook (ABA Publishing ed., 2d ed. 2017) (emphasis added)

HWG

Deepika H. Ravi
HWG, LLP
1919 M Street NW Suite 800
Washington, D.C. 20036
Office: 202.730.1353
dravi@hwglaw.com

Hilary P. Gerzhoy
HWG, LLP
1919 M Street NW Suite 800
Washington, D.C. 20036
Office: 202.730.1342
hgerzhoy@hwglaw.com