AMERICAN BANKRUPTCY INSTITUTE

2018 Mid-Atlantic Bankruptcy Workshop

Ethical Use of Artificial Intelligence/Technology in the Legal Industry

Scott Y. Stuart, Moderator
Esquify, Inc.; Chicago

Ericka F. Johnson
Womble Bond Dickinson (US) LLP; Wilmington, Del.

Mette H. Kurth
Fox Rothschild LLP; Wilmington, Del.

Hon. Henry W. Van Eck
U.S. Bankruptcy Court (M.D. Pa.); Harrisburg

PLENARY SESSION

2018

Ethical Use of Artificial Intelligence/Technology in the Legal Industry

1. What is Artificial Intelligence?
2. How is Artificial Intelligence Used in the Legal Industry?
3. Overview of Rules of Professional Responsibility that Impact Use of A.I./Tech in the Legal Industry
    a. **Rule 1.1 – Duty of Competence**
        i. Text:
            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.
        ii. Comment 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.
        iii. Cases:
            1. New Hampshire Bar Association Opinion #2012-13/4:

            As per Rule 1.1, "a competent lawyer using cloud computing must understand and guard against the risks inherent in it…The facts and circumstances of each case, including the type and sensitivity of client information, will dictate what reasonable protective measures a lawyer must take when using cloud computing…Competent lawyers must have a basic understanding of the technologies they use. Furthermore, as technology, the regulatory framework, and privacy laws keep changing, lawyers should keep abreast of these changes."

            2. New Hampshire Bar Association, Ethics Committee Opinion 2008-2009/4:

            In general, lawyers should be reasonably informed about the types of metadata that may be included in documents when they are transmitted electronically and the steps that can be taken to remove it, if necessary. Lawyers should stay abreast of technological advances and potential risks of transmission through appropriate training and education. In the Committee's view, lawyers should acquire, at the very least, a basic understanding of the existence of metadata embedded in electronic documents, the features of the software they have used to generate the document and any practical measures that may be taken to limit the likelihood of transmitting metadata or to purge the documents of sensitive information.

Of course, this does not mean that lawyers must necessarily purchase expensive computer software to ensure that metadata is removed or "scrubbed" from documents in all cases. In most circumstances, lawyers can limit the likelihood of transmitting metadata containing confidential information by avoiding its creation during document drafting or subsequently deleting it, as well as by sending a different version of the document without the embedded information through hard copy, scanned or faxed versions.

3. Vermont Bar Association, Ethics Opinion 2009-1:

The Bar Associations that have examined the duty of the sending lawyer with respect to metadata have been virtually unanimous in concluding that lawyers who send documents in electronic form to opposing counsel have a duty to exercise reasonable care to ensure that metadata containing confidential information protected by the attorney client privilege and the work product doctrine is not disclosed during the transmission process. See Alabama Ethics Op. RO 2007-02; Arizona Ethics Op. 07-03; Colorado Ethics Op. 119 (2008); DC Ethics Op. 341 (2007); Florida Ethics Op. 06-2; Maryland Ethics Op. 2007-09; New Hampshire Ethics Op. 2008-2009/4; New York City Lawyers Ass'n Ethics Op. No. 738 (2008); New York State Ethics Op. 782 (2004).

A number of other ethics opinions note that a sending lawyer has tools available to prevent against the risk of disclosing client confidences when electronic documents are transmitted to opposing counsel, but do not affirmatively address the scope of the sending lawyer's duty to take these steps. See Pennsylvania Formal Ethics Op. 2007-500; ABA Formal Ethics Op. 06-442.

This Opinion agrees that, based upon the language of the VRPC, a lawyer has a duty to exercise reasonable care to ensure that confidential information protected by the attorney client privilege and the work product doctrine is not disclosed. This duty extends to all forms of information handled by an attorney, including documents transmitted to opposing counsel electronically that may contain metadata embedded in the electronic file. This duty has its roots in VRPC 1.1, which requires lawyers to provide competent representation; VRPC 1.3, which requires lawyers to exercise diligence; and VRPC 1.6, which requires lawyers to protect confidential client information.

The Professional Responsibility Section notes that various tools are available to comply with this duty to exercise reasonable care, including programs to "scrub" metadata from electronic documents before they are dispatched, converting electronic documents to a read-only, PDF format before transmission, or insisting on transmission of

sensitive documents only on paper. The steps that should be taken by the sending lawyer in specific instances depend on the circumstances.

Reviewing the language of the Vermont Rules of Professional Conduct quoted above, the Vermont Bar Association Professional Responsibility Section finds nothing to compel the conclusion that a lawyer who receives an electronic file from opposing counsel would be ethically prohibited from reviewing that file using any available tools to expose the file's content, including metadata. A rule prohibiting a search for metadata in the context of electronically transmitted documents would, in essence, represent a limit on the ability of a lawyer diligently and thoroughly to analyze material received from opposing counsel.

4. Cloud Computing for Lawyers, TSUM04 ALI-CLE 1 (2012) - California State Bar, Formal Ethics Opinion 2010-179 (Dec. 2010):

Whether an attorney violates his or her duties of confidentiality and competence (Rules 1.1 and 1.6) when using technology to transmit or store confidential client information will depend on the particular technology being used and the circumstances surrounding such use. Before using a particular technology in the course of representing a client, an attorney must take appropriate steps to evaluate:

- the level of security attendant to the use of that technology, including whether reasonable precautions may be taken when using the technology to increase the level of security;
- the legal ramifications to a third party who intercepts, accesses or exceeds authorized use of the electronic information;
- the degree of sensitivity of the information;
- the possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product;
- the urgency of the situation; and
- the client's instructions and circumstances, such as access by others to the client's devices and communications.

5. Protecting Living Fossils: Crafting Technology Ethics Standards for the District of Columbia, 30 Geo. J. Legal Ethics 933 (Fall 2017):

   a. *In re Reisman,* 2013 WL 5967131 *1 (Ma. St. Bar Disp. Bd. 2013)

The case of In re Reisman depicts a lawyer who failed to recognize his own deficiencies and failed to consult someone familiar with the technology. In what could be considered a "light" e-discovery case, the disciplinary board for the state of Massachusetts sanctioned one of its lawyers in 2013 for failing to competently preserve data pursuant to an

injunction. In 2006, an employee of the lawyer's client brought his former work computer, supplied by and owned by his previous employer (the NSA), into the offices of his new employer, where he copied files of a confidential nature from his old computer onto his new one. Crucially, the lawyer instructed his client that it was acceptable for its employee to erase any files from the hard drive of his current work computer that had not originated with his first employer. The lawyer did not understand that the whole hard drive required preservation due to an existing court order granting access to the computer to an NSA investigator.

Although Massachusetts did not amend its rules to require technological competency until 2015, the Board of Bar Overseers Office of the Bar Counsel analyzed this case much as it might under a technological competence analysis, finding, for instance, that the sanctioned attorney had violated Rule 1.1.

The court faulted the lawyer for "handling a matter that he was not competent to handle without adequate research or associating with or conferring with experienced counsel, and without any attempt to confirm the nature and content of the proposed deletions."

b. *In re Collie,* 749 S.E.2d 522 (S.C. 2013).

In 2013, the state of South Carolina sanctioned a member of its bar for numerous transgressions that flowed from her failure to keep up with prevailing technology. It was discovered by the state Supreme Court that a woman representing herself in a 2012 case had not updated her contact information with the court, which in turn led to a series of missed communications from the court, as she failed to check her incoming email. Though she had been a member of the bar for more than thirty years, she had never practiced in the state except for the act of representing herself in the instant litigation. The court did not find that her semi-retired status was a mitigating factor.

The court's analysis reinforces the notion, expressed most strongly in the California Bar Opinion, that the duty to remain technologically competent (Rule 1.1) is a blanket duty that applies to all practicing lawyers even when the disciplined lawyer could not have harmed any party other than herself.

The lawyer in this case was handed an interim suspension by the court for failing to maintain and monitor an email account.

6. The Attorney's Ethical Obligations with Regard to the Technologies Employed in the Practice of Law, 29 Geo. J. Legal Ethics 849 (2016) - State Bar of Cal. Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. 2010-179 (2010)

The Standing Committee on Professional Responsibility evaluated the ethical duties related to technology that arise from a fairly common law firm arrangement--law-firm issued laptops that are used inside and outside the office and connected to public internet connections such as those found in coffee shops.

The committee concluded, "transmission of information through a third party [ISP] reasonably necessary for purposes of the representation should not be deemed to have destroyed the confidentiality of the information." (Rule 1.6) A lawyer may "meet the duty of [technological] competence (Rule 1.1) through association with another lawyer or consultation with an expert. Such expert may be an outside vendor, a subordinate attorney, or even the client, if they possess the necessary expertise." Although even when relying on experts, "[t]his consultation or association ... does not absolve an attorney's obligation to supervise the work of the expert under [the duty of competence], which is a non-delegable duty belonging to the attorney who is counsel in the litigation.

The committee outlines several factors a lawyer should consider before using a specific technology to meet his or her duties of confidentiality and competence. All attorneys, regardless of the size or nature of their practice should have the "ability to assess the level of security afforded by the technology:"

First, the practitioner should consider "how the particular technology differs from other media use."

Second, the practitioner should evaluate "[w]hether reasonable precautions may be taken when using the technology to increase the level of security." If an attorney can readily employ encryption when using public wireless connections and has enabled his or her personal firewall, the risks of unauthorized access may be significantly reduced." Further these steps are "readily available and relatively inexpensive." Additionally, the committee recommended enabling password features on laptops and PDAs to secure client information in the event of loss or theft.

Third, the lawyer should evaluate "who is permitted to monitor the use of the technology, to what extent and on what grounds." For example, the lawyer should determine that the technology's use or license agreements "do not permit the third party to disclose confidential client information to others or use such information for any purpose other than to ensure the functionality of the software or that the technology is not being used for an improper purpose." Additionally, "when a lawyer considers entering into a relationship with [] a service provider he must ensure that the service provider has in place, or will

establish, reasonable procedures to protect the confidentiality of information to which it gains access, and moreover, that it fully understands its obligations in this regard." Moreover, "[i]n connection with this inquiry, a lawyer might be well-advised to secure from the service provider in writing, along with or apart from any written contract for services that might exist, a written statement of the service provider's assurance of confidentiality."

Finally, the lawyer should consider the sensitivity of the information, the "[p]ossible impact on the client of an inadvertent disclosure of privileged or confidential information or work product," the necessity and urgency of using the technology, and client instructions and circumstances.

b. Rule 1.4 – Duty to Communicate

i. Text:

(a) A lawyer shall:

(1) promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(e), is required by these Rules;

(2) reasonably consult with the client about the means by which the client's objectives are to be accomplished;

(3) keep the client reasonably informed about the status of the matter;

(4) promptly comply with reasonable requests for information; and

(5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by the Rules of Professional Conduct or other law.

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

ii. Cases:

1. Vermont Bar Association, Ethics Opinion 2003-03:

A lawyer may engage an outside contractor as a computer consultant to recover a lost data-base file, which contains confidential client information so long as: The lawyer clearly communicates the confidentiality rules to the outside contractor; the contractor fully understands the confidentiality rules and embraces the obligation to maintain the confidentiality of any information obtained in the course of assisting the lawyer; and the lawyer determines that the contractor

has instituted adequate safeguards to preserve and protect confidential information. If a significant breach of confidentiality should occur by the outside contractor, the law firm would be obligated to disclose such a breach to the client.

For purposes of the Vermont Rules and in response to the pending inquiry, we believe that the requesting lawyer should follow a three-step process:

1. The lawyer must clearly explain the confidentiality rules to the contractor;

2. The contractor must fully understand the confidentiality rules and embrace the obligation to maintain the confidentiality of all information obtained in the course of assisting the lawyer.

3. The lawyer must determine that the contractor has instituted adequate safeguards to preserve and protect confidential information.

How a lawyer is to assure that a nonlawyer understands the obligation of confidentiality is not specifically spelled out in the Vermont Rules. Nonetheless, we believe that a lawyer would satisfy the reasonableness requirements of Rule 5.3 if the lawyer obtained a written acknowledgment from an outside contractor that the contractor understands the confidential nature of the material and understands his or her duty not to keep any information gained in strictest confidence. If a breach of confidentiality were to occur, RPC 1.4 requires a lawyer to explain a matter reasonably necessary to permit the client to make informed decision regarding representation. Thus, if the breach would affect the outcome of the client legal matter in any fashion, the lawyer would be obligated to tell the client of the breach by the nonlawyer.

2. *Jackson v. Lowe's Companies*, 2016 WL 6155937:

Plaintiff's counsel did not serve a copy of the motion to withdraw on the Plaintiff as required under Rule 1.4 using traditional methods of service. Plaintiff's counsel emailed the motion to withdraw to the Plaintiff and sent him text messages telling him to check his email. Nonetheless, the Court finds that Plaintiff's counsel properly served the Plaintiff.

Given the extraordinary occurrences here, including the fact that the Plaintiff moved to the Dominican Republic and refused to provide his new address; that the attorneys allegedly do not know the only mailing address in New York where the Plaintiff still receives mail; and that Plaintiff's counsel has previously corresponded with the Plaintiff via email; the Court finds that Plaintiff's counsel's efforts to serve the

Plaintiff through a known email address are sufficient to provide notice under Rule 1.4.

3. Cloud Computing for Lawyers, TSUM04 ALI-CLE 1 (2012) - ABA Standing Committee on Ethics and Professional Responsibility, Formal Opinion 11-459 (August 4, 2011):

   "Duty to Protect the Confidentiality of E-mail Communications with One's Client." (Rules 1.4 and 1.6)

   The opinion describes a situation where the lawyer has reason to believe that his or her client is transmitting confidential information via email in a situation where the client's employer has a monitoring system in place, such as a keylogger system, where there is a risk that the employer could access the client's confidential information. While this opinion on first glance covers the use of email only in workplace scenarios, the last paragraph of the opinion potentially broadens the scope to expand to other lawyer client communications. The opinion states:

   > [a] lawyer sending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, to which a third party may gain access. The risk may vary. Whenever a lawyer communicates with a client by e-mail, the lawyer must first consider whether, given the client's situation, there is a significant risk that third parties will have access to the communications. If so, the lawyer must take reasonable care to protect the confidentiality of the communications by giving appropriately tailored advice to the client.

4. VA Legal Eth. Op. 1872 (Virginia Legal Ethics Opinions), 2013 WL 6151724:

   If the communication will be conducted primarily or entirely electronically, the lawyer may need to take extra precautions to ensure that communication is adequate and that it is received and understood by the client…. A lawyer could permissibly represent clients with whom he had no in-person contact, because Rule 1.4 "in no way dictates whether the lawyer should provide that information in a meeting, in writing, in a phone call, or in any particular form of communication. In determining whether a particular attorney has met this obligation with respect to a particular client, what is critical is

what information was transmitted, not how." On the other hand, one of the aspects of communication required by Rule 1.4 is that a lawyer must "explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation." Use of the word "explain" necessarily implies that the lawyer must take some steps beyond merely providing information to make sure that the client actually is in a position to make informed decisions. A lawyer may not simply upload information to an Internet portal and assume that her duty of communication is fulfilled without some confirmation from the client that he has received and understands the information provided.

Finally, the technology that enables a lawyer to practice "virtually" without any face-to- face contact with clients can also allow lawyers and their staff to work in separate locations rather than together in centralized offices. As with other issues discussed in this opinion, a partner or other managing lawyer in a firm always has the same responsibility to take reasonable steps to supervise subordinate lawyers and nonlawyer assistants, but the meaning of "reasonable" steps may vary depending upon the structure of the law firm and its practice. Additional measures may be necessary to supervise staff who are not physically present where the lawyer works.

5. NY Eth. Op. 2014-2 (N.Y.St.Bar.Assn.Comm.Prof.Eth.), 2014 WL 11395033:

   Rule 1.4 requires lawyers to communicate with clients and keep them apprised of the status of their legal matters. Lawyers who use VLOs must be particularly mindful of these ethical obligations, given that the lawyers may frequently be away from the physical location that serves as their business address. Lawyers who use VLOs should also take steps to ensure that they are available to meet with and communicate with their clients and respond promptly to their requests for information.

6. PA Eth. Op. 2010-200 (Pa.Bar.Assn.Comm.Leg.Eth.Prof.Resp.), 2010 WL 11221119:

   An attorney maintaining a Virtual Law Office (VLO) may have unique communication considerations that attorneys in traditional physical offices do not face. For example, because the lawyer may only communicate with a client by email, the lawyer must take appropriate steps to confirm that the client has read and understands the information provided. (Rule 1.4).

c. Rule 1.5(a) – Attorney may not charge unreasonable fee

i. Text:

(a) A lawyer shall not make an agreement for, charge, or collect an unreasonable fee or an unreasonable amount for expenses. The factors to be considered in determining the reasonableness of a fee include the following:
(1) the time and labor required, the novelty and difficulty of the questions involved, and the skill requisite to perform the legal service properly;
(2) the likelihood, if apparent to the client, that the acceptance of the particular employment will preclude other employment by the lawyer;
(3) the fee customarily charged in the locality for similar legal services;
(4) the amount involved and the results obtained;
(5) the time limitations imposed by the client or by the circumstances;
(6) the nature and length of the professional relationship with the client;
(7) the experience, reputation, and ability of the lawyer or lawyers performing the services; and
(8) whether the fee is fixed or contingent.

d. Rule 1.6(a) – Duty of Confidentiality

i. Text:

(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).

ii. Cases:

1. VA Legal Eth. Op. 1872 (Virginia Legal Ethics Opinions), 2013 WL 6151724:

Acting competently to protect the confidentiality of clients' information is more difficult when the information is being transmitted and/or stored electronically through third- party software and storage providers. 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. 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.

2. Massachusetts Bar Association, Opinion 12-03 (March 2012):

   A lawyer generally may store and synchronize electronic work files containing confidential client information across different platforms and devices using an Internet based storage solution, such as "Google docs," so long as the lawyer undertakes reasonable efforts to ensure that the provider's terms of use and data privacy policies, practices and procedures are compatible with the lawyer's professional obligations, including the obligation to protect confidential client information reflected in Rule 1.6(a). A lawyer remains bound, however, to follow an express instruction from his or her client that the client's confidential information not be stored or transmitted by means of the Internet, and all lawyers should refrain from storing or transmitting particularly sensitive client information by means of the Internet without first obtaining the client's express consent to do so.

3. North Carolina 2011 Formal Opinion #6 (January 27, 2012):

   While the duty of confidentiality applies to lawyers who choose to use technology to communicate, "this obligation does not require that a lawyer use only infallibly secure methods of communication." Rather, the lawyer must use reasonable care to select a mode of communication that, in light of the circumstances, will best protect confidential client information and the lawyer must advise effected parties if there is reason to believe that the chosen communications technology presents an unreasonable risk to confidentiality. (Rule 1.6)

   In light of the above, the Ethics Committee concludes that a law firm may use [cloud computing] . . . if reasonable care is taken to minimize the risks of inadvertent disclosure of confidential information and to protect the security of client information and client files. A lawyer must fulfill the duties to protect confidential client information and to safeguard client files by applying the same diligence and competency to manage the risks of [cloud computing] . . . that the lawyer is required to apply when representing clients.

4. New Hampshire Bar Association Opinion #2012-13/4:

   Cloud computing comes into wider use, storing and transmitting information in the cloud may be deemed an impliedly authorized disclosure to the provider, so long as the lawyer takes reasonable steps to ensure that the provider of cloud computing services has adequate safeguards…Not all information is alike. For example, where highly sensitive data is involved, it may become necessary to inform the

client of the lawyer's use of cloud computing and to obtain the client's informed consent.

5. Vermont Bar Association, Ethics Opinion 2009-1:

> The Bar Associations that have examined the duty of the sending lawyer with respect to metadata have been virtually unanimous in concluding that lawyers who send documents in electronic form to opposing counsel have a duty to exercise reasonable care to ensure that metadata containing confidential information protected by the attorney client privilege and the work product doctrine is not disclosed during the transmission process. *See* Alabama Ethics Op. RO 2007-02; Arizona Ethics Op. 07-03; Colorado Ethics Op. 119 (2008); DC Ethics Op. 341 (2007); Florida Ethics Op. 06-2; Maryland Ethics Op. 2007-09; New Hampshire Ethics Op. 2008-2009/4; New York City Lawyers Ass'n Ethics Op. No. 738 (2008); New York State Ethics Op. 782 (2004).
>
> A number of other ethics opinions note that a sending lawyer has tools available to prevent against the risk of disclosing client confidences when electronic documents are transmitted to opposing counsel, but do not affirmatively address the scope of the sending lawyer's duty to take these steps. *See* Pennsylvania Formal Ethics Op. 2007-500; ABA Formal Ethics Op. 06-442.
>
> This Opinion agrees that, based upon the language of the VRPC, a lawyer has a duty to exercise reasonable care to ensure that confidential information protected by the attorney client privilege and the work product doctrine is not disclosed. This duty extends to all forms of information handled by an attorney, including documents transmitted to opposing counsel electronically that may contain metadata embedded in the electronic file. This duty has its roots in VRPC 1.1, which requires lawyers to provide competent representation; VRPC 1.3, which requires lawyers to exercise diligence; and VRPC 1.6, which requires lawyers to protect confidential client information.
>
> The Professional Responsibility Section notes that various tools are available to comply with this duty to exercise reasonable care, including programs to "scrub" metadata from electronic documents before they are dispatched, converting electronic documents to a read-only, PDF format before transmission, or insisting on transmission of sensitive documents only on paper. The steps that should be taken by the sending lawyer in specific instances depend on the circumstances.
>
> Reviewing the language of the Vermont Rules of Professional Conduct quoted above, the Vermont Bar Association Professional Responsibility Section finds nothing to compel the conclusion that a

lawyer who receives an electronic file from opposing counsel would be ethically prohibited from reviewing that file using any available tools to expose the file's content, including metadata. A rule prohibiting a search for metadata in the context of electronically transmitted documents would, in essence, represent a limit on the ability of a lawyer diligently and thoroughly to analyze material received from opposing counsel.

6. A Lawyer's Duty to Clients, Elect. Disc. L. & Pract. 5622329 (C.C.H.), 2015 WL 5622329 - *In re Peshek, Ill. Attorney Registration and Disciplinary Comm'n, Commission* No. 09CH89 (Aug. 25, 2009)

   A lawyer was found to have violated Illinois Professional Conduct Rule 1.6, based on numerous comments the lawyer posted on her blog regarding her work as a public defender. The disciplinary commission determined that in her work-related blogs, the lawyer disclosed 'confidential information about [the lawyer's] clients and [made] derogatory comments about judges.' Among other things, the lawyer 'referred to her clients by either their first name, a derivative of their first name, or by their jail identification number.'

7. Cloud Computing for Lawyers, TSUM04 ALI-CLE 1 (2012):

   a. ABA Standing Committee on Ethics and Professional Responsibility, Formal Opinion 11-459 (August 4, 2011)

   "Duty to Protect the Confidentiality of E-mail Communications with One's Client." (Rules 1.4 and 1.6)

   The opinion describes a situation where the lawyer has reason to believe that his or her client is transmitting confidential information via email in a situation where the client's employer has a monitoring system in place, such as a keylogger system, where there is a risk that the employer could access the client's confidential information. While this opinion on first glance covers the use of email only in workplace scenarios, the last paragraph of the opinion potentially broadens the scope to expand to other lawyer client communications. The opinion states:

   > [a] lawyer sending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, to which a third party may gain access. The risk may vary. Whenever a lawyer communicates with a client by e-mail, the lawyer must first consider whether, given the client's situation, there is a significant risk that third parties will have access to the

communications. If so, the lawyer must take reasonable care to protect the confidentiality of the communications by giving appropriately tailored advice to the client.

b. *California State Bar, Formal Ethics Opinion 2010-179 (December 2010):*

Whether an attorney violates his or her duties of confidentiality and competence (Rules 1.1 and 1.6) when using technology to transmit or store confidential client information will depend on the particular technology being used and the circumstances surrounding such use. Before using a particular technology in the course of representing a client, an attorney must take appropriate steps to evaluate:

1) the level of security attendant to the use of that technology, including whether reasonable precautions may be taken when using the technology to increase the level of security;

2) the legal ramifications to a third party who intercepts, accesses or exceeds authorized use of the electronic information;

3) the degree of sensitivity of the information;

4) the possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product;

5) the urgency of the situation; and

6) the client's instructions and circumstances, such as access by others to the client's devices and communications.

8. The Attorney's Ethical Obligations with Regard to the Technologies Employed in the Practice of Law, 29 Geo. J. Legal Ethics 849 (2016):

a. *N.Y. State Bar Ass'n Comm. on Professional Ethics, Opinion 820 (2008)*

In 2008, the New York State Bar Association Committee on Professional Ethics revisited email and considered the use of email service providers that scan emails for advertising purposes. In the instances at issue, email providers were using computer programs to scan the user's mail, looking for keywords in order to provide targeted advertising. The analysis focused on the email provider's privacy policy that stated the content of the emails were not read by any humans other than the sender and the intended recipient. The committee reasoned, "[m]erely scanning the content of e-mails by computer to generate computer advertising, however, does not pose a threat to client confidentiality, because the practice does not increase

the risk of others obtaining knowledge of the e-mails or access to the e-mails' content."

Therefore, the committee found the use of email providers that employ automated scanning of emails did not violate the duty to preserve client confidentiality (Rule 1.6). The committee was quick to note that the opposite conclusion would have been reached had humans read the emails "or if the service provider reserved the right to disclose the e-mails or the substance of the communications to third parties without the sender's permission." Finally, the committee charged lawyers with a duty to exercise due care in selecting email providers and evaluating their privacy policies and practices.

b. *State Bar of Cal. Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. 2010-179 (2010)*

The Standing Committee on Professional Responsibility evaluated the ethical duties related to technology that arise from a fairly common law firm arrangement--law-firm issued laptops that are used inside and outside the office and connected to public internet connections such as those found in coffee shops.

The committee concluded, "transmission of information through a third party [ISP] reasonably necessary for purposes of the representation should not be deemed to have destroyed the confidentiality of the information." (Rule 1.6) A lawyer may "meet the duty of [technological] competence (Rule 1.1) through association with another lawyer or consultation with an expert. Such expert may be an outside vendor, a subordinate attorney, or even the client, if they possess the necessary expertise." Although even when relying on experts, "[t]his consultation or association ... does not absolve an attorney's obligation to supervise the work of the expert under [the duty of competence], which is a non-delegable duty belonging to the attorney who is counsel in the litigation.

The committee outlines several factors a lawyer should consider before using a specific technology to meet his or her duties of confidentiality and competence. All attorneys, regardless of the size or nature of their practice should have the "ability to assess the level of security afforded by the technology:"

First, the practitioner should consider "how the particular technology differs from other media use." Second, the practitioner should evaluate "[w]hether reasonable precautions may be taken when using the technology to increase the level of security." If an attorney can readily employ encryption when using public wireless connections and has enabled his or her personal firewall, the risks of unauthorized access may be significantly reduced." Further these steps are "readily

available and relatively inexpensive." Additionally, the committee recommended enabling password features on laptops and PDAs to secure client information in the event of loss or theft. Third, the lawyer should evaluate "who is permitted to monitor the use of the technology, to what extent and on what grounds." For example, the lawyer should determine that the technology's use or license agreements "do not permit the third party to disclose confidential client information to others or use such information for any purpose other than to ensure the functionality of the software or that the technology is not being used for an improper purpose." Additionally, "when a lawyer considers entering into a relationship with [] a service provider he must ensure that the service provider has in place, or will establish, reasonable procedures to protect the confidentiality of information to which it gains access, and moreover, that it fully understands its obligations in this regard." Moreover, "[i]n connection with this inquiry, a lawyer might be well-advised to secure from the service provider in writing, along with or apart from any written contract for services that might exist, a written statement of the service provider's assurance of confidentiality." Finally, the lawyer should consider the sensitivity of the information, the "[p]ossible impact on the client of an inadvertent disclosure of privileged or confidential information or work product," the necessity and urgency of using the technology, and client instructions and circumstances.

e. Rule 2.1 – Lawyer as counselor

i. Text:

1. In representing a client, a lawyer shall exercise independent professional judgment and render candid advice. In rendering advice, a lawyer may refer not only to law but to other considerations such as moral, economic, social and political factors, that may be relevant to the client's situation.

ii. Case:

1. New Hampshire Bar Association Opinion #2012-13/4:

Under Rule 2.1, a lawyer must exercise independent professional judgment in representing a client and cannot hide behind a hired intermediary and ignore how client information is stored in or transmitted through the cloud…It bears repeating that a lawyer's duty is to take reasonable steps to protect confidential client information, not to become an expert in information technology. When it comes to the use of cloud computing, the Rules of Professional Conduct do not impose a strict liability standard."

f. Rules 5.1-5.3 – Duty of Supervision

i. Text:

1. Rule 5.1 –
    a. A partner in a law firm, 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 all lawyers in the firm conform to the Rules of Professional Conduct.
    b. A lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct.
    c. A lawyer shall be responsible for another lawyer's violation of the Rules of Professional Conduct if:
        i. the lawyer orders or, with knowledge of the specific conduct, ratifies the conduct involved; or
        ii. the lawyer is a partner or has comparable managerial authority in the law firm in which the other lawyer practices, or has direct supervisory authority over the other lawyer, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.
2. Rule 5.2 –
    a. A lawyer is bound by the Rules of Professional Conduct notwithstanding that the lawyer acted at the direction of another person.
    b. A subordinate lawyer does not violate the Rules of Professional Conduct if that lawyer acts in accordance with a supervisory lawyer's reasonable resolution of an arguable question of professional duty.
3. Rule 5.3 –

    With respect to a nonlawyer 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 nonlawyer 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:
    i. the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or
    ii. 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.

ii. Cases:

1. NY Eth. Op. 2014-2 (N.Y.St.Bar.Assn.Comm.Prof.Eth.), 2014 WL 11395033:

Under Rules 5.1 and 5.3, law firms and lawyers are responsible for supervising the conduct of subordinate lawyers and nonlawyers and ensuring that their conduct complies with the Rules. These obligations apply to attorneys who use Virtual Law Offices (VLOs). *See* Cal. Op. 2012-184, 2012 WL 3182985, at *7 (noting that "in all law offices, including this hypothetical VLO, attorneys have a duty to supervise subordinate attorneys, and non-attorney employees or agents"). Given the differences between a VLO and a traditional law office, however, it may be more challenging for lawyers who use VLOs to comply with their supervisory obligations. As explained in Cal. Op. 2012-184, "supervision [in the context of a VLO] can be a challenge if Attorney and her various subordinate attorneys and employees operate out of several different physical locations." *Id.* Furthermore, as a practical matter, lawyers have less control over the conduct of VLO personnel than they would over their own direct employees in a conventional physical law firm office. Thus, lawyers who use VLOs may need to take additional precautions to ensure that they are fulfilling their supervisory obligations. Notwithstanding the differences between VLOs and traditional law firms, the "[a]ttorney must take reasonable measures to ascertain that everyone under her supervision is complying with the Rules of Professional Conduct, including the duties of confidentiality and competence." *Id.* at *7.

A lawyer who uses the shared services and office space of a VLO to perform legal services and to meet with clients, witnesses, or other third parties must take reasonable steps to ensure that she does not expose or put the client's confidential information at risk. This should include, as appropriate, training and educating staff at the VLO on these obligations. *See* Rule 5.3(a) (requiring lawyers to supervise the work on nonlawyers).

2. PA Eth. Op. 2010-200 (Pa.Bar.Assn.Comm.Leg.Eth.Prof.Resp.), 2010 WL 11221119:

It is likely in a VLO that a supervisory lawyer may not be practicing in the same building (or perhaps the same city or county) as subordinate lawyers over whom the lawyer has a duty of supervision. In these circumstances, a supervisory lawyer must "make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct."

3. Connecticut Bar Association, Informal Opinion 2013-07 (June 19, 2013):

Cloud computing online outsourcing is subject to Rule 5.1 and Rule 5.3 governing the supervision of those who are hired by and associated with the lawyer. Therefore, a lawyer must ensure that tasks are delegated to competent and reliable people and organizations. This means that the lawyer outsourcing cloud computing tasks (of transmitting, storing and processing data) must exercise reasonable efforts to select a cloud service provider whose conduct is compatible with the professional obligations of the lawyer and is able to limit authorized access to the data, ensure that the data is preserved ("backed up"), reasonably available to the lawyer, and reasonably safe from unauthorized intrusion.

4. New Hampshire Bar Association, Ethics Committee Opinion 2008-2009/4:

Lawyers should consider the duty to provide competent representation under Rule 1.1, as well as the general requirement under Rules 5.1 and 5.3 that lawyers make reasonable efforts to ensure that their firms, including lawyers and non-lawyers, conform to the Rules. In general, lawyers should be reasonably informed about the types of metadata that may be included in documents when they are transmitted electronically and the steps that can be taken to remove it, if necessary. Lawyers should stay abreast of technological advances and potential risks of transmission through appropriate training and education. In the Committee's view, lawyers should acquire, at the very least, a basic understanding of the existence of metadata embedded in electronic documents, the features of the software they have used to generate the document and any practical measures that may be taken to limit the likelihood of transmitting metadata or to purge the documents of sensitive information.

Of course, this does not mean that lawyers must necessarily purchase expensive computer software to ensure that metadata is removed or "scrubbed" from documents in all cases. In most circumstances,

lawyers can limit the likelihood of transmitting metadata containing confidential information by avoiding its creation during document drafting or subsequently deleting it, as well as by sending a different version of the document without the embedded information through hard copy, scanned or faxed versions.

5. New Hampshire Bar Association Opinion #2012-13/4:

As per Rule 5.3(a) (Responsibilities Regarding Nonlawyer Assistants), "Cloud computing is a form of outsourcing the storage and transmission of data…[W]hen, instead of directly engaging a cloud computing provider, a lawyer hires an intermediary, such as an information technology professional or other support staff, to find and engage a provider…When engaging a cloud computing provider or an intermediary who engages such a provider, the responsibility rests with the lawyer to ensure that the work is performed in a manner consistent with the lawyer's professional duties. Rule 5.3 (a). Additionally, under Rule 2.1, a lawyer must exercise independent professional judgment in representing a client and cannot hide behind a hired intermediary and ignore how client information is stored in or transmitted through the cloud…It bears repeating that a lawyer's duty is to take reasonable steps to protect confidential client information, not to become an expert in information technology. When it comes to the use of cloud computing, the Rules of Professional Conduct do not impose a strict liability standard."

6. NHBA Ethics Committee, #2012-13/05 Social Media Contact with Witnesses in the Course of Litigation:

May the lawyer's client send a Facebook friend request or request to follow a restricted Twitter feed, and then reveal the information learned to the lawyer? The answer depends on the extent to which the lawyer directs the client who is sending the request. Rule 8.4(a) prohibits a lawyer from accomplishing through another that which would be otherwise barred. Also, while Rule 5.3 is directed at legal assistants rather than clients, to the extent that the client is acting as a non-lawyer assistant to his or her own lawyer, Rule 5.3 requires the lawyer to advise the client to avoid conduct on the lawyer's behalf which would be a violation of the rules.

Subject to these limitations, however, if the client has a Facebook or Twitter account that reasonably reveals the client's identity to the witness, and the witness accepts the friend request or request to follow a restricted Twitter feed, no rule prohibits the client from sharing with the lawyer information gained by that means. In the non-social media context, the American Bar Association has stated that such contact is permitted in similar limitations. See ABA Ethics Opinion 11-461.7

The non-lawyer assistant is subject to the same restrictions as the lawyer. The lawyer has a duty to make sure the assistant is informed about these restrictions and to take reasonable steps to ensure that the assistant acts in accordance with the restrictions. Thus, if the non-lawyer assistant identifies him- or herself, the lawyer, the client, and the cause in litigation, then the non-lawyer assistant may properly send a social media request to an unrepresented witness.

7. Vermont Bar Association, Ethics Opinion 2003-03:

A lawyer may engage an outside contractor as a computer consultant to recover a lost data-base file, which contains confidential client information so long as: The lawyer clearly communicates the confidentiality rules to the outside contractor; the contractor fully understands the confidentiality rules and embraces the obligation to maintain the confidentiality of any information obtained in the course of assisting the lawyer; and the lawyer determines that the contractor has instituted adequate safeguards to preserve and protect confidential information. If a significant breach of confidentiality should occur by the outside contractor, the law firm would be obligated to disclose such a breach to the client.

For purposes of the Vermont Rules and in response to the pending inquiry, we believe that the requesting lawyer should follow a three-step process:

1. The lawyer must clearly explain the confidentiality rules to the contractor;

2. The contractor must fully understand the confidentiality rules and embrace the obligation to maintain the confidentiality of all information obtained in the course of assisting the lawyer.

3. The lawyer must determine that the contractor has instituted adequate safeguards to preserve and protect confidential information.

How a lawyer is to assure that a nonlawyer understands the obligation of confidentiality is not specifically spelled out in the Vermont Rules. Nonetheless, we believe that a lawyer would satisfy the reasonableness requirements of Rule 5.3 if the lawyer obtained a written acknowledgment from an outside contractor that the contractor understands the confidential nature of the material and understands his or her duty not to keep any information gained in strictest confidence. If a breach of confidentiality were to occur, RPC 1.4 requires a lawyer to explain a matter reasonably necessary to permit the client to make informed decision regarding representation. Thus, if the breach would affect the outcome of the client legal matter in any fashion, the lawyer would be obligated to tell the client of the breach by the nonlawyer.

g. Rule 5.5(a) – Unauthorized Practice of Law

i. Text

1. A lawyer shall not practice law in a jurisdiction in violation of the regulation of the legal profession in that jurisdiction, or assist another in doing so.

ii. Cases:

1. Artificial Intelligence: State of the Industry and Ethical Issues, 54-Mar Tenn. B.J. 24 (2018) - *Reynoso v US,* 477 F.3d 1117 (9th Cir. 2007)

In 2007, the Ninth Circuit held that a software called the Ziinet Bankruptcy Engine, which offered **automated bankruptcy assistance**, constituted the **unauthorized** practice of law (Rule 5.5):

> The software did, indeed, go far beyond providing clerical services. It determined where (particularly, in which schedule) to place information provided by the debtor, selected exemptions for the debtor and supplied relevant legal citations. Providing such personalized guidance has been held to constitute the practice law [The] system touted its offering of legal advice and projected an aura of expertise concerning bankruptcy petitions; and, in that context, it offer personalized--albeit automated--counsel. We find that because this was the conduct of a non-attorney, it constituted the unauthorized practice of law.

2. Artificial Intelligence: Ethics Issues, TSZJ10 ALI-CLE 1 (February 22, 2018) - *LegalZoom.com, Inc., v. N.C. State Bar*, 2015 NCBC 96 ¶¶ 1, 2 (N.C. Super. Ct. Oct. 22, 2015)

The parties agree that the definition of the 'practice of law' (Rule 5.5) as set forth in N.C.G.S. § 84-2.1 does not encompass LegalZoom's operation of a website that offers consumers access to interactive software that generates a legal document based on the consumer's answers to questions presented by the software so long as LegalZoom complies with the below provisions:

> "(a) LegalZoom shall provide to any consumer purchasing a North Carolina product (a North Carolina Consumer) a means to see the blank template or the final, completed document before finalizing a purchase of that document";
>
> "(b) An attorney licensed to practice law in the State of North Carolina has reviewed each blank template

offered to North Carolina Consumers, including each and every potential part thereof that may appear in the completed document. The name and address of each reviewing attorney must be kept on file by LegalZoom and provided to the North Carolina Consumer upon written request"

"(c) LegalZoom must communicate to the North Carolina Consumer that the forms or templates are not a substitute for the advice or services of an attorney";

"(d) LegalZoom discloses its legal name and physical location and address to the North Carolina Consumer";

"(e) LegalZoom does not disclaim any warranties or liability and does not limit the recovery of damages or other remedies by the North Carolina Consumer; and

(f) LegalZoom does not require any North Carolina Consumer to agree to jurisdiction or venue in any state other than North Carolina for the resolution of disputes between LegalZoom and the North Carolina Consumer."