International Franchise Association
51st Annual Legal Symposium
May 6-8, 2018
Washington, DC

Ethics and the Cloud, A Lawyer's Dilemma

(How Painful Can Colliding with a Cloud Be?)

Michael R. Daigle, Esq.
Cheng Cohen, LLC
Chicago, Illinois

Sharon Nelson, Esq.
President, Sensei Enterprises, Inc.
Fairfax, Virginia

Erika Stillabower, Esq.
Senior Legal Ethics Counsel, District of Columbia Bar
Washington, D.C.

TABLE OF CONTENTS

I. What is Cloud Computing?

Cloud computing is merely "a fancy way of saying stuff's not on your computer."[1] That is a great way, in plain English, to define the playing field, but the Pennsylvania Bar Association's Formal Opinion 2011-200, as did many other ethics opinions summarized below, provided a more formal definition as well: "'Cloud computing' encompasses several similar types of services under different names and brands, including: web-based e-mail, online data storage, software-as-a-service ('SaaS'), platform-as-a-service ('PaaS'), infrastructure-as-a-service ('IaaS'), Amazon Elastic Cloud Compute ('Amazon EC2'), and Google Docs." Precisely. The stuff's not on your computer, but you and perhaps your clients use your (or their) computer or other electronic device to access it.

The Pennsylvania Bar Association's Formal Opinion 2011-200 also summed it up in this way:

> [Cloud computing] refers to software and related services that store information on a remoted computer, i.e., a computer or server that is not located at the law office's physical location. Rather, the information is stored on another company's server, or many servers, possibly all over the world, and the user's computer becomes just a way of accessing the information.

and:

> If an attorney uses a Smartphone or an iPhone, or uses web-based electronic mail (e-mail) such as Gmail, Yahoo!, Hotmail or AOL Mail, or uses products such as Google Docs, Microsoft Office 365 or Dropbox, the attorney is using 'cloud computing.'

If the "stuff" is not on your computer, then where is it? It's most likely stored on large servers – or "server farms" – that might or might not be located in the United States and, if not located in the US, might or might not be subject to the same level of protection as is data that is housed in the US. In the following sections, we look at lawyers' professional responsibility obligations applicable to their use of the cloud. As is apparent from the ethics opinions discussed below, exercising "reasonable care" to protect the confidentiality of client information is a fairly uniform standard, so it is not unreasonable to expect that part of exercising that level of care would require a lawyer to have some degree of understanding about the location of data and, if not in the US, the extent to which it is protected under the laws of the jurisdiction in which it is stored. More on that in later sections of this paper.

Any study of lawyers and the cloud will yield a few themes. First, more than ever, clients (who often are also under obligations with respect to protection of some of the same data that they will communicate to their lawyers) are insisting that their lawyers

[1] Quinn Norton, "Byte Rights," *Maximum PC*, September 2010, at 12. Cited by the Pennsylvania Bar Association's Committee on Legal Ethics and Professional Responsibility in its Formal Opinion 2011-200 (copy attached to this paper as Appendix A).

establish data security policies and procedures to ensure that their information, and perhaps their own clients' or customers' information in the hands of the lawyer, is secure and reasonably protected from improper disclosure or illegal interception. Second, people who are looking for ways to get their hands on information and data for their own illicit and illegal use are finding that it is often more efficient – easier, faster and less expensive – to hack a law firm than it is to have the company directly. As a result, the FBI has been warning law firms for at least a decade regarding data intrusions, and several major law firms have been in the news in the past few years for being hacked by people who wanted to get their hands on information about the firm's clients that they could then use to make trades on relevant stock exchanges. And finally, data security is an enterprise issue and, as such, requires the involvement of everyone in the enterprise.

The focus of this paper is on the ethical considerations that impact lawyers' use of cloud computing. That is a small part of the issues around data security that, if fully understood and complied with, could play a large and integral role in the protection of data generally.

II. How Are the Rules of Professional Conduct Implicated?

The American Bar Association's Model Rules of Professional Conduct mention technology only once, and that reference came about in an August 2012 amendment to the Model Rules in which Comment 8 to Rule 1.1 was amended to read as follows (language added in the amendment is underscored):

> To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, <u>including the benefits and risks associated with relevant technology</u>, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

While the fact that the Model Rules provide only that single reference to technology might seem odd at first blush, a review of the ethics opinions issued by the ethics committees of the various states' Bar Associations (discussed below) nicely illustrate the rationale. In its opinion, the Professionalism Committee of the Ohio Bar Association noted that the storage of client files in the cloud is analogous to storage of those files in an off-site brick and mortar location owned and operated by a third-party.[2] That opinion, as did the opinions rendered by several other states' ethics committees, noted that the issue should be viewed as merely applying old principles to new technology – in other words, the technology impacts how the lawyer approaches his or her ethical obligations, but it does not alter the lawyer's fundamental obligations.

The two most prevalent professional responsibility concepts implicated in cloud computing are "competence" and "confidentiality." It makes complete sense - by using

[2] Informal Opinion 2013-003 issued by the Professionalism Committee of the Ohio Bar Association, Issued July 25, 2013.

a third-party cloud service provider, the lawyer is entrusting the client's confidential file information to a third-party, and it must do so competently while taking reasonable steps to ensure the continued confidentiality of those materials. However, other concepts also come into play, in particular: supervision of non-lawyer agents, client's informed consent, and safeguarding client property.

Following are the rules of the Model Rules of Professional Conduct and their comments that are recognized in the various ethics opinions to be implicated by a lawyer's use of third-party cloud computing providers.[3] Following each Rule and applicable Comments, the authors of this paper have noted the context in which the Rule and Comments are most often cited in the ethics opinions summarized in Section III below when discussing in those opinions a lawyer's professional responsibilities regarding cloud computing:

Model Rule 1.1 (Competence):

> *A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.*
>
> Applicable Comment to Model Rule 1.1:
>
> *[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.*

Note: This Rule and Comment are most often cited in the context of the lawyer's obligations to use reasonable care in understanding the technology, in selecting the third-party cloud service provider, and in contracting with the provider.

Model Rule 1.4 (Communication)

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

Note: This Rule is most often cited in the context of the lawyer's obligation to ensure that the client understands that the lawyer will use cloud computing technology, the risks associated with that use (for example, communications being subject to

[3] References are to the current version of the ABA's Model Rules of Professional Conduct. As they are adopted by the various states, the actual rule number may vary, but, in most cases, the substance is substantially the same and the correlation to the Model Rules is apparent. However, not all states have adopted the Model Rules and comments in their entirety. Interestingly, when some of the ethics committees' opinions discussed in Section III below were issued, their particular state had not yet modified their rules to include the reference noted above to "technology" in Comment 8 to Model Rule 1.1. The conclusions of the various ethics committees, however, did not appear to be affected by whether or not that reference had been so incorporated.

interception by third-parties and information being subject to hacking), and obtaining the client's informed consent to that use, particularly with respect to extraordinarily sensitive information and communications.

Model Rule 1.6 (Confidentiality of Information):

> *(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).*
>
> ....
>
> *(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.*

Applicable Comments to Model Rule 1.6:

Acting Competently to Preserve Confidentiality

[18] Paragraph (c) requires a lawyer to act competently 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). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with non-lawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].

[19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This

duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

Note: This Rule and applicable Comments are most often cited as perhaps the largest risk to one of the lawyer's most fundamental obligations to his or her client.

Model Rule 1.15 (Safekeeping Property)

(a) *A lawyer shall hold property of clients or third persons that is in a lawyer's possession in connection with a representation separate from the lawyer's own property....*

Note: This Rule is most often cited in the context of the lawyer's obligation to ensure that the client's file materials are safe, secure, and always available.

Model Rule 4.4 (Respect for Rights of Third Persons)

(b) 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 was inadvertently sent shall promptly notify the sender.

Applicable Comments to Rule 4.4:

[2] Paragraph (b) recognizes that lawyers sometimes receive a document or electronically stored information that was mistakenly sent or produced by opposing parties or their lawyers. A document or electronically stored information is inadvertently sent when it is accidentally transmitted, such as when an email or letter is misaddressed or a document or electronically stored information is accidentally included with information that was intentionally transmitted. If a lawyer knows or reasonably should know that such a document or electronically stored information was sent inadvertently, then this Rule requires the lawyer to promptly notify the sender in order to permit that person to take protective measures. Whether the lawyer is required to take additional steps, such as returning the document or electronically stored information, is a matter of law beyond the scope of these Rules, as is the question of whether the privileged

status of a document or electronically stored information has been waived. Similarly, this Rule does not address the legal duties of a lawyer who receives a document or electronically stored information that the lawyer knows or reasonably should know may have been inappropriately obtained by the sending person. 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.

[3] Some lawyers may choose to return a document or delete electronically stored information unread, for example, when the lawyer learns before receiving it that it was inadvertently sent. Where a lawyer is not required by applicable law to do so, the decision to voluntarily return such a document or delete electronically stored information is a matter of professional judgment ordinarily reserved to the lawyer. See Rules 1.2 and 1.4.

Note: This Rule and applicable Comments are most often cited in the context of a lawyer's inadvertent receipt of metadata or other client communications that are electronically transmitted through the use of e-mail and third-party providers such as Dropbox.

Model Rule 5.1 (Responsibilities of a Partner or Supervisory Lawyer):

(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:

(1) the lawyer orders or, with knowledge of the specific conduct, ratifies the conduct involved; or

(2) the lawyer is a partner or has comparable managerial authority in the law firm in which the 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.

Model Rule 5.2 (Responsibilities of a Subordinate Lawyer):

> *(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.*

Model Rule 5.3 (Responsibilities Regarding Non-Lawyer Assistance):

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

Note: Rules 5.1, 5.2 and 5.3 are most often cited in the context of the lawyer's obligation to fully vet third-party cloud computing providers before handing over to the third-party the client files with which the lawyer has been entrusted. While acknowledging that the lawyer is not a guarantor of the people with whom he or she works, the opinions summarized in Section III below are clear that the lawyer must use reasonable care in selecting the provider, in obtaining the agreement of the provider with respect to confidentiality of the client's materials, in ensuring the provider's ability to make the client's file materials available, and in addressing the disposition of the client's file materials on termination or expiration of the agreement with the provider.

III. How Have State Bar Associations Responded?

As of the date of this paper, less than half the states' Bar Associations have issued opinions on a lawyer's use of cloud computing and the impact of doing so on the lawyer's ethical obligations, particularly the obligations of competency and confidentiality. Those that have issued opinions did so in the early part of this century, and they tend to rely heavily on each other. Their opinions, being so fundamentally consistent, are instructive for lawyers in all states (which might explain why so many states have yet to opine on the issue). The states that have issued opinions consistently opine that the use of cloud computing does not violate the ethics rules provided that the lawyer uses reasonable care in selecting, contracting with, and using third-party cloud data providers. While they reach essentially the same conclusions, the analysis and recommendations in each are worth consideration. While some summarize and rely on opinions rendered in other states, they come from different perspectives, and each would seem to be helpful to lawyers in any state attempting to meet their ethical obligations in the cloud computing arena.

Following is a list of states that, as of the date of this paper, have issued formal or informal opinions on the issue and, for each, a summary of the opinion. It should be noted that, for the most part, these opinions are advisory (not binding) and, because of the rapidity of technological changes, acknowledge that what is "reasonable care" today may not be so as those changes occur.

ALABAMA – Formal Opinion 2010-02

This Opinion notes, as its premise, that Rule 1.15 of Alabama's Rules of Professional Conduct impose on the lawyer an obligation to safeguard a client's property. The client's files must be secured, and reasonable measures must be taken to protect the confidentiality, security and integrity of the client's file documents. The lawyer must ensure that the process is at least as secure as required for traditional paper files, but should also ensure that only authorized persons have access and that the files are secure from outside intrusion (for example, by installing firewalls and intrusion detection software). The Opinion also states that the lawyer should back-up all electronically stored files onto another computer or media in case of computer crashes, file corruption or physical damage.

The Opinion accepts that lawyers will face physical space limitations and have access to technological alternatives, but recognizes that, through electronic or cloud-based storage, client confidences will no longer be under the lawyer's direct control and will become open to the possibility that a third-party could illegally gain access to the servers and to confidential client data. The Opinion further recognizes that, as is true with paper files, there is no guarantee against a breach of confidence, but it imposes on the lawyer an obligation to use reasonable care when using third-party providers or internet-based servers and in selecting and entrusting confidential client data to third-party vendors. Reasonable care, in that context, includes:

- becoming knowledgeable about how the third-party vendor will handle storage and security,
- reasonably ensuring that the vendor will abide by an obligation to maintain the confidentiality of client data, and
- satisfying a continuing duty to stay abreast of constantly evolving technology.

The Opinion further notes that the lawyer storing client files electronically must be able to reproduce documents in their original paper format and, when discarding computers, must take adequate measures to ensure that all client data is appropriately erased from the discarded hardware.

ARIZONA – Opinions 07-02, 05-04, and 09-04

The State Bar of Arizona (SBA), in Opinion 05-04, opined that electronic storage of client files is permissible as long as lawyers and law firms "take competent and reasonable steps to assure that the client's confidences are not disclosed to third parties through theft or inadvertence." In making that determination, the SBA relied primarily on ER 1.6 regarding confidentiality, which provides: "A lawyer must act competently to safeguard information relating to the representation of a client 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." In Opinion 09-04, it responded to an inquiry by a lawyer regarding the sufficiency of a system that uses encryption and three layers of unique randomly generated alpha-numeric folder names and passwords. It also noted that the inquiring lawyer had taken the preliminary step of having the files protected by a Secure Socket Layer (SSL) server, which encrypts the files, applied several layers of password protection, and used a system that also utilizes unique and randomly generated folder names and passwords, all of which appear to satisfy the requirement of taking reasonable measures to protect client confidentiality and prevent unauthorized access of confidential client data. In opining that the system appeared to satisfy the "reasonable steps" requirement, the SBA noted, however, that reasonableness must be assessed based on the state of the technology at any given time. Thus, it noted, the lawyer will have a continuing responsibility, using competent personnel, to conduct periodic reviews to ensure that security precautions in place remain reasonable as technology progresses.

CALIFORNIA – Formal Opinion 2010-179

The State Bar of California (SBC) considered the issue of whether a lawyer violates the duties of confidentiality and competence by using technology to transmit or store confidential client information in the context of a lawyer's conducting research and emailing his client via the internet using public wi-fi access provided by a local coffee shop and his personal wi-fi connection at his home. The SBC first looked at the lawyer's absolute obligation under Rule 3-100 of California's Rules of Professional Conduct to maintain the confidentiality of client information, but noted that the

transmission of that information (to/from the client, to opposing counsel, etc.) requires the placement of the information into the hands of third-parties (for example, postal workers in the case of mailings of paper copies). Noting that such transmission will not destroy the attorney-client privilege under the rules of evidence, it stated: "While the duty to protect confidential client information [under the Rules of Professional Responsibility] is broader in scope than the attorney-client privilege ..., the underlying principle remains the same, namely, that transmission of information through a third party reasonably necessary for purposes of the representation should not be deemed to have destroyed the confidentiality of the information." The SBC then examined the relationship to the issue of the lawyer's duties under Rule 3-110 of the California Rules of Professional Conduct of competency and supervision of subordinate attorneys and non-attorney employees or agents. The SBC listed several factors that it believes are relevant to an assessment of the lawyer's compliance with these duties in this context: (1) the lawyer's ability to assess the level of security afforded by the technology, (2) legal ramifications to third parties of intercepting, accessing or exceeding authorized use of another person's electronic information (noting, for example, the fact that hackers can be criminally charged reinforces the expectation of privacy), (3) the degree of sensitivity of the information, (4) the possible impact on the client of an inadvertent disclosure of privileged or confidential information (for example, potential waiver of the attorney-client privilege), (5) the urgency of the situation, and (6) client instructions and circumstances. It is worth noting that the SBC devoted considerable space to the factors that are relevant to the assessment of the technology's level of security:

- Consideration of how the particular technology differs from other media use.

- Whether reasonable precautions may be taken when using the technology to increase the level of security (for example, use of firewalls and password protocols)

- Limitations on who is permitted to monitor the use of the technology, to what extent and on what grounds. Notable here is the lawyer's obligation to ensure that a third-party technology provider will agree to treat the information as confidential and to put in place safeguards to protect and limit accessibility to confidential information.

The SBC noted that while lawyers are not necessarily tech-savvy and excused them from developing a mastery of the security features of each technology, it provided a reminder of the duty under Rule 3-110(C) of the California Rules of Professional Conduct to consult with someone who does and noted that "the duties of confidentiality and competence that attorneys owe to their clients do require a basic understanding of the electronic protections afforded by the technology they use in their practice."

Applying these principles to the scenario at hand, the SBC advised that the lawyer's accessing the internet via his personal home wi-fi would likely be acceptable as long as appropriate firewalls and security measures are in place. However, it advised that use of the public wi-fi access provided by the local coffee shop could be problematic given the lack of appropriate security measures available in such public access unless the

lawyer uses his own security measures (for example, file encryption and personal firewalls that would be installed on the laptop). Without those security measures, the lawyer may need to avoid the public wi-fi or duly inform the client of the associated risks and secure the client's informed consent.

CONNECTICUT – Informal Opinions 99-52 and 2013-07

In its January 2013 informal opinion, the Professional Ethics Committee of the Connecticut Bar Association considered whether it is permissible under the Connecticut Rules of Professional Responsibility for a lawyer to use cloud computing in the practice of law. It immediately recognized the requirement that the lawyer "keep pace" with what is – and will be – a constantly changing environment. Its opinion spanned cloud computing (which it defined as "the storage, transmission, and processing of client information and data using shared computer facilities owned or leased by a third party service provider), the use of Software as a Service (SaaS) applications that operate on a cloud infrastructure which may be located at remote sites in and outside of Connecticut (including in foreign countries), using third-party services for online storage of data, and online transmission of client data through email service providers like gmail.

In its opinion, the Committee noted that it is ultimately the responsibility of the user of the technology (the lawyer, not the provider), to ensure the privacy and security of the client data and information stored or transmitted through the cloud service, and that "lawyers who use cloud computing have a duty to understand its potential impact on their obligations under applicable law and under the Rules of Professional Responsibility." Citing its 1999 opinion and the lawyer's obligation under Rule 1.15 of the Connecticut Rules of Professional Responsibility to safeguard client information, the CBA recognized that it is the lawyer's responsibility to ensure that the transmission, storage and possession of the client's data does not diminish the lawyer's "ownership of and unfettered accessibility to the data" and that the provider's security policies and mechanisms segregate the lawyer's data and prevent unauthorized access, including by the cloud service provider itself. The opinion further referenced the lawyer's obligation under Rule 5.1 and Rule 5.3 to adequately supervise those who are hired by or associated with the lawyer.

FLORIDA – Opinions 10-2 and 12-3

In Florida Ethics Opinion 12-3, the Professional Ethics Committee of the Florida Bar, the Committee cited the lawyer's obligation under Rule 4-1.6 of the Rules Regulating The Florida Bar to maintain the confidentiality of client information by the lawyer and by non-lawyers under the lawyer's supervision or used by the lawyer in the provision of legal services. It opined that lawyers who use cloud computing must take reasonable precautions to protect the confidentiality of that information, ensure that the third-party provider of cloud services it uses maintains adequate security, and ensure that the lawyer has adequate remote access to the information. The Opinion relied on Florida Ethics Opinion 10-2 that had previously confirmed the lawyer's obligation to stay current on technology advances that impacted the practice of law, and agreed, in particular,

with the positions and advice given by their Iowa and New York counterparts (see below) on the same issue.

IOWA – Opinion 11-01

In September 2011, the Ethics and Practice Guidelines Committee of the Iowa Bar Association opined on the use by lawyers of Software as a Service (SaaS applications in the practice of law. The Committee noted that, unlike software that is housed on the lawyer's computer, SaaS is a subscription-bases application that allows the lawyer to access files and data over the internet via a web browser, with upgrades and updates being rolled out continuously. Because client information is stored on computer services that are not owned or operated by the lawyer, Rule 32:1.6 of the Iowa Rules of Professional Conduct (confidentiality) and, in particular, comment 17 to that Rule, are brought into play. The Opinion recognizes that the degree of protection of client information in connection with the use of SaaS will vary depending on the client, the matter, and the information involved; but what doesn't vary is the lawyer's obligation to perform due diligence to assess the degree of protection that will be needed and to act accordingly. In that context, the Committee focused on two key factors: accessibility and data protection. The Opinion suggests that lawyers intending to use, or using, an SaaS ask the following questions:

- Will I have access to the stored data, including via another source if access through the SaaS is denied?
- Have I performed due diligence on the provider of the SaaS? Due diligence should include:
    - What is the provider's operating history?
    - Is the service recommended by those who have used it?
    - Where will the data actually be stored (in what state, in what country)?
    - In the provider's End User License Agreement, does the provider agree to confidentiality and the lawyer's ownership (as between the lawyer and the provider) of the stored information?
- What is the cost of the service, and what happens if I default in the payment of the subscription fee? Is my access to or ownership of the data impacted?
- How do I terminate the provider and, upon termination, retrieve my data in a useable form and format? Does the provider retain copies?
- How will the provider protect my data?
- If I allow someone to access a portion of my data, will other portions be protected from view?

- Will I have the ability to select higher level encryption for data that is more sensitive?

The Committee noted that due diligence on the SaaS provider must be performed by individuals with the required level of technology expertise and an understanding of the Iowa Rules of Professional Conduct, but it accepted that the lawyer may discharge its due diligence duties by relying on independent companies, bar associations or other similar organizations, or through its own qualified employees.

MAINE – Opinions #194 and #207

Opinion #194 of the Professional Ethics Commission of the Maine Board of Bar Overseers laid the groundwork for a cloud computing opinion when it addressed the ethics of a lawyer's transmitting dictated recordings for transcription by third-parties. In its Opinion #207, the Commission elected to squarely address the issue of whether it is ethical for lawyers to use cloud computing and storage for client matters. It opined that it is, provided that safeguards are in place to ensure that the lawyer's use of this technology does not result in the violation of any of the lawyer's obligations under the various Maine Rules of Professional Conduct. The Commission noted that the constantly changing technology does not change the lawyer's ethical obligation but, rather, changes the way in which those constraints are satisfied when technology is used in the practice of law.

In drawing on the opinions of the ABA and other states' bar associations (particularly, Pennsylvania and North Carolina, discussed below), the Commission noted that, reasonable care, not infallibility, is the standard and developed several safeguards that it believed Maine lawyers should adopt when using cloud computing and storage (quoted below from Opinion #207):

- Back up data to allow the firm to restore data that has been lost, corrupted, or accidentally deleted;
- Install a firewall to limit access to the firm's network;
- Limit information that is provided to others to what is required, needed, or requested;
- Avoid inadvertent disclosure of information;
- Verify the identity of individuals to whom the attorney provides confidential information;
- Refuse to disclose confidential information to unauthorized individuals (including family members and friends) without client permission;
- Protect electronic records containing confidential data, including backups, by encrypting the confidential data;

- Implement electronic audit trail procedures to monitor who is accessing the data;

- Create plans to address security breaches, including the identification of persons to be notified about any known or suspected security breach involving confidential data; and

- Educate and train employees of the firm who use cloud computing to abide by all end-user security measures, including, but not limited to, the creation of strong passwords and the regular replacement of passwords.

- In dealing with third-party vendors of cloud computing services or hardware:

    - Include in the vendor's Terms of Service or Service Level Agreement, or in a separate agreement between the vendor and the lawyer or law firm, an agreement on how the vendor will handle confidential client information in keeping with the lawyer's professional responsibilities.

    - Ensure that, if the agreement with the vendor is terminated, the vendor goes out of business, or the service otherwise has a break in continuity, the law firm will have a method for retrieving the data in a non-proprietary format that the law firm can access, or the firm will have access to the vendor's software or source code.

    - The vendor should be contractually required to return or destroy the hosted data promptly at the request of the law firm.

    - The lawyer should conduct a careful review of the terms of the law firm's user or license agreement with the vendor including the security policy.

    - The lawyer should evaluate the vendor's (or any third party data hosting company's) measures for safeguarding the security and confidentiality of stored data including, but not limited to, firewalls, encryption techniques, socket security features, and intrusion-detection systems.

    - The lawyer should evaluate the extent to which the vendor backs up hosted data.

    - There should be an explicit agreement from the provider that it has no ownership or security interest in the data; that it has an enforceable obligation to preserve security; that it will notify the lawyer if requested to produce data to a third party, and provide the lawyer with the ability to respond to the request before the provider produces the requested information; that it has technology built to withstand a reasonably foreseeable attempt to infiltrate data,

including penetration testing; that it provides the firm with the right to audit the provider's security procedures and to obtain copies of any security audits performed; that it will host the firm's data only within a specified geographic area (if the data is hosted outside of the United States, the law firm must determine that the hosting jurisdiction has privacy laws, data security laws, and protections against unlawful search and seizure that are as rigorous as those of the United States and Maine); and that it provides the ability for the law firm, on demand, to get data from the vendor's or third-party data hosting company's servers for the firm's own use or for in-house backup.

MASSACHUSETTS – Opinions 00-01, 05-04 and 12-03

In its earlier opinion (Opinion 00-01), the Committee on Professional Ethics had concluded that sending unencrypted emails did not necessarily violate Rule 1.6(a) of the Massachusetts Rules of Professional Conduct (duty to protect confidential client information) because, even though there was a possibility that the emails could be intercepted, that same risk was present with respect to other forms of communication, and it did not destroy the parties' expectation of privacy.

In Opinion 05-04, the Committee opined that a lawyer did not violate Rule 1.6(a) by providing a third-party vendor with access to its own servers (which contained client information) for the purposes of having them serviced by the vendor as long as the lawyer used reasonable efforts to ensure that the vendor would act in a manner that was compatible with the lawyer's ethical obligations regarding the confidentiality of the client's information.

In its most recent opinion (Opinion 12-03), the Committee further opined that a lawyer generally may use cloud computing (such as Google docs) to store and synchronize electronic work files containing confidential client information "*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." What would constitute "reasonable efforts" in the Committee's view, focus on the agreement between the lawyer and the vendor to include those expressed provisions that would require the vendor to act in a way that is compatible with the lawyer's ethical obligations (for example, agreements in the license or subscription agreement for the vendor to acknowledge a confidentiality obligation and to install and maintain security measures consistent with that obligation). It looked specifically at the terms of service agreement used by Google docs and concluded that they appear to be consistent with the lawyer's obligations (noting, however, that its opinion was merely advisory and that whether it was appropriate for the lawyer to use Google docs was a matter to be determined in a specific case in another forum).

Finally, the Opinion further suggests that, because the lawyer must nevertheless act in accordance with its client's instruction should the client elect not to have its

information stored or transmitted by means of the internet, the lawyer should obtain the client's express consent before storing or transmitting particularly sensitive client information by means of the internet.

NEW HAMPSHIRE – Opinion #2012-13/04

In this Opinion, the Ethics Committee of the New Hampshire Bar Association confirmed its agreement with the position taken by bar associations of other states regarding the ability of lawyers to use cloud computing and opined that "while a lawyer need not become an expert in data storage, a lawyer must remain aware of how and where data is stored and what the service agreement says" and otherwise use reasonable efforts to ensure the confidentiality of the client's sensitive confidential information.

Relying principally on Rule 1.0(e) (informed consent), Rule 1.1 (competence), Rule 1.6 (confidentiality), Rule 1.15 (safekeeping of client property), and Rule 5.3 (requirements regarding non-lawyer assistants), the Committee opined that the lawyer should:

- inform the client of its use of technology and the risks associated therewith, and obtain the client's expressed consent to the use of technology to store and transmit its information
- stay abreast of technology changes
- conduct due diligence in selecting, contracting with, and training the cloud vendor with respect to confidentiality and maintenance of the client's information and files

NEW JERSEY – Opinion 701

In considering the question of whether a lawyer could "digitize" his files (in this case, save them as pdf files and store them electronically), the Advisory Committee on Professional Ethics turned to Rule 1.6 (confidentiality) and, in particular, the lawyer's obligation to "exercise reasonable care" against the possibility of unauthorized access to the client's information. Noting that "reasonable care" does not mean an absolute guarantee that the client's information will be safe from unauthorized access, the Committee recognized that compliance with the standard will be judged by the advancements in the technology that is used by the lawyer. It noted that reasonable care will have been satisfied if: (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 (for example, in the case of a pdf of a sensitive document, the lawyer should password protect the document).

NEW YORK – Opinions 709 and 842

In Opinion 709 (1998), New York's Committee on Professional Ethics opined that the transmission of client files via email would not violate Rule 1.6 (confidentiality) but cautioned that lawyers should assess the particular sensitivity of the particular documents when deciding whether to do so. So, for example, transmission via an unencrypted email might not be appropriate when the contents of the documents being transmitted are of an extraordinarily sensitive nature.

In September 2010, the Committee considered, in the context of Rule 1.6 (confidentiality) whether a lawyer could use an online system to store a client's confidential information and, if so, what steps the lawyer should take to ensure that the information is reasonably secure. The Committee noted that, while the obligation of confidentiality applies with respect to the lawyer's own actions, the lawyer is also obligated under Rule 1.6(c) to "exercise reasonable care to prevent . . . others whose services are utilized by the lawyer from disclosing or using confidential information of a client." It opined that a lawyer may use an online "cloud" backup system to store client files provided that the lawyer takes reasonable care to ensure that the system is secure and that client confidentiality will be maintained. It suggested that "reasonable care" may include the following (quoting from the Opinion):

- ensuring that the online data storage provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information;
- investigating the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances;
- employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored; and/or
- investigating the storage provider's ability to purge and wipe any copies of the data, and to move the data to a different host, if the lawyer becomes dissatisfied with the storage provider or for other reasons changes storage providers.

NEVADA – Opinion 33

In this Opinion, rendered in February 2006, the State Bar of Nevada's Standing Committee on Ethics and Professional Responsibility discussed whether a lawyer violates Supreme Court Rule 156 (confidentiality) by, without the client's consent, storing client information on a third-party server which is not owned by the lawyer and over which the lawyer has no direct control. It determined that, where the lawyer acted competently and reasonably in protecting the information from inadvertent and unauthorized disclosure, it would not violate SCR 156. Drawing

from the ABA's position, the Committee noted that the lawyer will not be in violation where it (1) uses reasonable care in selecting the provider, (2) has a reasonable expectation that the information will not be disclosed, and (3) instructs and requires the provider to keep the information confidential and inaccessible to unauthorized persons.

NORTH CAROLINA – 2011 Formal Ethics Opinion 6

In January 2012, the Ethics Committee of the North Carolina State Bar opined that a law firm that uses SaaS in its practice has a dual obligation of taking steps to minimize risk of inadvertent or unauthorized disclosure of client information and to protect the client's file from risk of loss, in either case, "applying the same diligence and competency to manage the risks of SaaS that the lawyer is required to apply when representing clients." The Committee recognized that it would be imprudent to hand down specific steps that should be taken to minimize risks of disclosure or loss of client information and data given the speed at which technology changes. It did, however, recommend that the lawyer take certain steps when assessing the vendor (note: many of these concepts embody the same suggestions that were adopted by Maine, discussed above):

- Include in the SaaS vendor's Terms of Service or Service Level Agreement, or in a separate agreement between the SaaS vendor and the lawyer or law firm, of an agreement on how the vendor will handle confidential client information in keeping with the lawyer's professional responsibilities.

- If the lawyer terminates use of the SaaS product, the SaaS vendor goes out of business, or the service otherwise has a break in continuity, the law firm should have a method for retrieving the data in a non-proprietary format that the law firm can access, or the firm should have access to the vendor's software or source code. The SaaS vendor should be contractually required to return or destroy the hosted data promptly at the request of the law firm.

- Careful review of the terms of the law firm's user or license agreement with the SaaS vendor including the security policy.

- Evaluation of the SaaS vendor's (or any third party data hosting company's) measures for safeguarding the security and confidentiality of stored data including, but not limited to, firewalls, encryption techniques, socket security features, and intrusion-detection systems.

- Evaluation of the extent to which the SaaS vendor backs up hosted data.

OHIO – Informal Advisory Opinion 2013-03

In this 2013 Opinion, the Professionalism Committee of the Ohio Bar Association noted that a lawyer's ethical duties regarding cloud storage are analogous to the duties that apply to a lawyer who uses off-site storage of client's paper files, and lawyers have

always been under a duty to make reasonable judgments when protecting client property and information. So it viewed this issue as merely applying old principles to new technology – in other words, the technology does not change the lawyer's ethical obligation, but it clearly impacts how the lawyer approaches the obligation. Against that backdrop, the Committee noted what by now should be easily recognizable as the four common issues in applying Ohio's Rules of Professional Conduct to storing a client's information on the cloud: (1) selecting the cloud provider, (2) preserving confidentiality and safeguarding client property, (3) supervising the cloud provider, and (4) communicating with the client. Fundamental to these issues is the notion that client files are the client's property, entrusted to the lawyer during the course of the representation. The lawyer's obligation, therefore, is to protect the property that doesn't belong to him and, when he places that property in the hands of a third-party, the lawyer must exercise reasonable care in doing so.

OREGON – Formal Opinion No. 2011-188 [Revised 2015]

The Oregon Board of Governors approved and adopted this Opinion stating that a lawyer may store client information on a third-party server as long as the lawyer complies with his or her obligations of competence and confidentiality to "reasonably keep the client's information secure within a given situation." The Opinion further noted that the lawyer must take reasonable steps to ensure that the third-party vendor will reliably secure the client's data and keep the client's information confidential, measured against the technology then available. That would likely require that the lawyer stay abreast of technological advancements and to periodically reevaluate how and to what extent the vendor is able to protect the client's information.

PENNSYLVANIA – Formal Opinion 2011-200

The Committee on Legal Ethics and Professional Responsibility of the Pennsylvania Bar Association concluded in this Opinion that lawyers should be able to take advantage of cloud services in an effort to promote mobility, flexibility, efficiencies and cost reductions. However, in doing so, the lawyer "must be conscientious about maintaining traditional confidentiality, competence and supervisory standards." The Opinion is one of the most detailed and illustrative of all, capturing many of the standards that have been adopted by other states' bar associations. For that reason, a copy of the Opinion is attached to this paper as Appendix A.

Of note, the Opinion recognizes that, in many instances, cloud vendors store data (or back-up data) outside the United States. While that might be permissible in the context of the lawyer's compliance with his or her ethical obligations, it imposes an additional wrinkle that requires the lawyer to ensure that the privacy laws of the country in which the data is stored "reasonably mirror" those of the United States.

VERMONT – Opinion 2010-6

The Professional Responsibility Section of the Vermont Bar Association considered the use of SaaS by a law firm and, in this Opinion, relied heavily on the opinions of other

states' bar associations to conclude that Vermont lawyers may do so as long as they take reasonable precautions to protect the confidentiality of and to ensure access to the client's materials. While noting that it would be inappropriate to establish a firm set of requirements (due to the changing nature of the technology), the Section concluded that complying with the required level of due diligence would require an understanding by the lawyer of:

- the vendor's security system;
- what practical and foreseeable limits, if any, may exist to the lawyer's ability to ensure access to, protection of, and retrieval of the data;
- the material terms of the user agreement;
- the vendor's commitment to protecting confidentially of the data;
- the nature and sensitivity of the stored information;
- notice provisions if a third party seeks or gains (whether inadvertently or otherwise) access to the data; and
- other regulatory, compliance, and document retention obligations that may apply based upon the nature of the stored data and the lawyer's practice.

In addition, it suggested that the lawyer should consider:

- giving notice to the client about the proposed method for storing client data;
- having the vendor's security and access systems reviewed by competent technical personnel;
- establishing a system for periodic review of the vendor's system to be sure the system remains current with evolving technology and legal requirements; and
- taking reasonable measures to stay apprised of current developments regarding SaaS systems and the benefits and risks they present.

VIRGINIA – Legal Ethics Opinion 1872

This Opinion considered the issue of cloud computing in the context of a virtual law office (which, by definition, are "in the cloud") and executive office suites, and, like other states, concluded that cloud computing is permissible subject to the lawyer's obligation to "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 Opinion further notes that, given the need of the lawyer to assess the vendor's ability to provide adequate security measures, the lawyer should have the assessment done by a qualified third-party if he or she feels unqualified to do so.

WASHINGTON – Advisory Opinion 2215

In 2012, the Committee on Professional Ethics of the Washington State Bar Association considered the implications of Rules 1.1, 1.6, and 1.5(a) of Washington's Code of Professional Conduct where a law firm contracts with a third-party vendor to store client files and documents on a remote server so that the lawyer and the client could access the documents over the internet from any remote location. Applying the competence and confidentiality provisions, the Committee noted that "a lawyer must act competently to safeguard information relating to the representation of a client 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 also Comment [18] discussed in Section II above in connection with Model Rule 1.6).

Opining that cloud computing would be permissible as long as the lawyer exercises reasonable care and competence, the Committee listed several best practices for a lawyer without advanced technological knowledge:

- Familiarization with the potential risks of online data storage and review of available general audience literature and literature directed at the legal profession, on cloud computing industry standards and desirable features.
- Evaluation of the provider's practices, reputation and history.
- Comparison of provisions in service provider agreements to the extent that the service provider recognizes the lawyer's duty of confidentiality and agrees to handle the information accordingly.
- Comparison of provisions in service provider agreements to the extent that the agreement gives the lawyer methods for retrieving the data if the agreement is terminated or the service provider goes out of business.
- Confirming provisions in the agreement that will give the lawyer prompt notice of any non-authorized access to the lawyer's stored data.
- Ensure secure and tightly controlled access to the storage system maintained by the service provider.
- Ensure reasonable measures for secure backup of the data that is maintained by the service provider.

WISCONSIN – Opinion EF-15-01

The Professional Ethics Committee of the State Bar of Wisconsin expressed a view that, consistent with other states, acknowledges that it is permissible for lawyers to use cloud computing as long as he or she uses reasonable efforts to adequately address the associated risks. It further noted that what is "reasonable" is measured against the risks presented.

IV. A Word About Metadata

Metadata is data, typically found embedded in documents, that provides information about other data,[4] often including the identity of the person who created the document, the date it was created, and even a short summary of the document and its various versions. Metadata might, in some cases, itself be highly sensitive and confidential, and it could even be used against a lawyer's client. When documents are sent electronically by a lawyer without scrubbing metadata, he risks having breached his obligation of confidentiality. As a result, several state ethics committees have addressed the issue, particularly in the context of a potential violation of Model Rule 1.6. In addition to the ABA, 20 states have specifically addressed the lawyer's responsibility with respect to metadata: Alabama, Arizona, Colorado, Florida, Maine, Maryland, Minnesota, Mississippi, New Hampshire, New York, North Carolina, Oregon, Pennsylvania, Vermont, Washington, Washington DC, West Virginia, and Wisconsin.

The opining states uniformly agree that the transmitting lawyer has an obligation under their state's equivalent of Model Rule 1.6 to take reasonable steps to remove unwanted metadata from documents before they are transmitted, and that receiving lawyers who inadvertently discover metadata in documents they receive should notify the transmitting lawyer of their discovery (Oregon clearly disagrees with that notion). The states are less aligned when it comes to the issue of whether a receiving attorney is allowed to mine for metadata in documents they receive from opposing counsel. Most opined that lawyers should not mine documents for metadata, but those that disagreed often qualified their positions by opining that special software should not be used for that purpose. An invaluable resource on this topic is the ABA's publication "Metadata Ethics Opinions Around the US" found at:

https://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/metadatachart.html.

V. Other Electronic and "Net" Based Issues

The internet plays into the practice of law in many more ways that can be addressed in this paper and, while many of them are outside the scope of this paper, some are worth noting.

- "Friending" an Adversary. In Opinion 2014-5, the Committee on Professional Ethics of the Massachusetts Bar Association examined the question of whether a lawyer may "friend" an unrepresented adversary on the adversary's non-public social media site for the purpose of obtaining information from the adversary. The Committee opined that the lawyer could do so only if the lawyer has been able to send a message that discloses his or her identity as the other party's lawyer.

[4] This is the standard Merriam Webster definition of the term.

- Investigating a Witness Via Social Media. The Ethics Committee of the New Hampshire Bar Association, in Opinion 2012-13/05, opined that the Rules of Professional Conduct do not forbid a lawyer's use of social media to investigate a non-party witness so long as the lawyer follows the same rules that would apply in other contexts (particularly, truthfulness, fairness, and respect for the rights of third parties). The Committee noted that the lawyer's sending a message through social media with just the lawyer's name might not be enough to inform the witness of the lawyer's identity or his role in the pending litigation.

- Internet Posting as an Inadvertent Waiver of Privilege. The issue of inadvertent waiver of attorney/client privilege became the subject of litigation when a lawyer posted an insurance company's claims file to a publicly accessible folder on the internet.[5] The case arose out of a suspicious fire at a funeral home. The merits of the civil case between the funeral home and its insurer were stayed pending the disposition of a related criminal prosecution. The issue regarding waiver of the attorney/client privilege stems from the following facts:

    - In the early stages of the investigation, the insurance company's parent was communicating with the National Insurance Crime Bureau (NICB) regarding the fire. As part of those communications, an investigator for the insurance company's parent uploaded to a "Box Folder" (an internet-based file sharing service) surveillance video footage of the fire scene. He then sent an email to an NICB agent with a "sharing" link to the Box Folder that contained the uploaded footage. The email was designated as "privileged and confidential."

    - Some seven months later, the investigator for the insurance company's parent was asked to send the insurance company's claims file and the parent company's investigation file to the insurance company's counsel. The agent uploaded both files to the same Box Folder and sent the insurer's lawyer an email with what he failed to realize was the same "sharing" link that he had previously provided to NICB some seven months earlier. The result was that NICB, a non-party to the litigation, had access to the Box Folder that, at one time, had only the video surveillance footage but that now housed the entire claims and investigative files of the insurer and its parent. NICB, however, had not accessed the Box Folder since it did so to retrieve the surveillance video footage.

    - The funeral home's counsel issued a subpoena duces tecum to NICB requesting that NICB turn over to the insurer its entire file relating to the fire. Among the documents produced by NICB was the original email from the insurer's parent's investigator with the link to the Box Folder. The funeral home's counsel used the link to access the Box Folder and found

[5] Harleysville Insurance Company vs. Holding Funeral Home, Inc., et al., Case No. 1:15CV00057, United States District Court, W.D. Virginia, Abingdon Division

that the folder contained the entire claims and investigations files, with many documents marked "confidential" and "privileged."

- The funeral home's counsel incorrectly assumed that the insurance company's counsel had provided its claims and investigative files to NICB, a third-party, and assumed that the insurance company had, therefore, waived the attorney/client privilege with respect to the claims and investigative file materials.

- The funeral home's counsel contacted the Virginia State Bar's ethics hotline for advice on how to proceed and conducted its own research. Since it assumed that the attorney/client privilege had been waived, it continued its review of the claims and investigative files and did not notify the insurance company's counsel that it was in possession of those materials. It also did not seek the court's ruling on the waiver issue.

- The insurance company's counsel sought to disqualify the funeral home's counsel. The magistrate judge denied the motion, finding that the insurance company waived the privilege when it uploaded the files to a publicly accessible, non-password-protected-website.

The District Court reversed on the privilege waiver issue, finding that the disclosure of the privileged materials was inadvertent and that the privilege was not waived because the insurance company had taken reasonable precautions to safeguard the files and preserve their confidentiality.[6] The decision is a good reminder to counsel of the importance of remaining diligent when using these types of cloud storage vehicles, how they are used and to whom the log-in link is provided.

- **AVVO and Other Lawyer Directories**. While several states' ethics committees have opined that online directories that list the lawyer's name, basic information such as bar admissions, and practice area are generally permissible,[7] lawyers should be extra careful when "claiming" listings that go beyond providing such basic information. Lawyers are often solicited by companies who operate "free" online directories (for example, AVVO) and are asked to "claim" their listing as written or to make changes. The listing then includes a description of the lawyer's practice, a star-based rating for the lawyer based on peer reviews, and a section on which peers and clients are able to post "reviews" regarding the lawyer's performance. The South Carolina Bar Association, in Ethics Advisory Opinion 09-10, considered whether lawyers may, without violating the state's Rules of Professional Conduct, are permitted to "claim" their listing and to invite peers and clients to submit reviews has cautioned lawyers. The Opinion states

[6] The District Court noted that the Box Folder was not searchable through a search engine and that the "sharing" link needed to access the folder consisted of 32 randomly-generated alphanumeric characters (functioning like a password).

[7] See, for example, State Bar of Arizona Ethics Opinion 99-10 and Massachusetts Bar Association Committee on Professional Ethics Op. 98-2 (May 1998).

that lawyers may "claim" their listings and invite ratings and reviews, but once they do, they become responsible for the content of the listing and, thus, for ensuring that the listing otherwise complies with the Rules of Professional Conduct, especially with respect to lawyer advertising, communications, and testimonials. The Opinion specifically called out services such as AVVO, Martindale-Hubbell, SuperLawyers, and LinkedIn and stated that "regardless of the terminology, by requesting access to and updating any website listing (beyond merely making corrections to directory information), a lawyer assumes responsibility for the content of the listing."

- **International Travel and Electronic Devices**. In January 2018, the American Bar Association issued an Executive Summary intended for lawyers traveling to its Mid-Year Meeting in Vancouver, specifically discussing the Model Rules of Professional Responsibility in relation to carrying electronic devices in international travel and the potential for those devices to be searched during travel.[8] The Executive Summary noted that attendees and their electronic devices are subject to search both when leaving and when re-entering the United States[9] and advised that lawyers exercise special caution when traveling with electronic devices that contain confidential client information to avoid violating the Rules of Professional Conduct, particularly those pertaining to competence (Rule 1.1), client confidentiality (Rule 1.6), supervisory responsibilities (Rules 5.1 and 5.3) and communications (Rule 1.4) all of which are discussed in Section II of this paper.

  The Executive Summary referenced a 2017 opinion issued by the New York City Bar Association (Formal Ethics Opinion 2017-5) that indicated that compliance with the demands of a border agent to search the lawyer's electronic device would not violate Rule 1.6 on confidentiality provided the lawyer first attempts, using reasonable efforts, to dissuade the border agent from reviewing the lawyer's client's confidential information. The Executive Summary concluded by suggesting that attendees to the Mid-Year Meeting consider doing several things, including:

  - Leave electronic devices at home

---

[8] Found electronically at https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/scepr_electronic_device_advisory_exec_summary.authcheckdam.pdf. The Executive Summary was prepared by Hon. Daniel J. Crothers, Justice of the Supreme Court of North Dakota, and Barbara S. Gillers, Adjunct Professor of Law at New York University School of Law.

[9] The Executive Summary makes specific reference to the broad search powers given to US Customs and Border Protection officers under a Directive issued by the US Customs and Border Protection Agency on January 4, 2018, that applies specifically to searches of electronic devices. The Directive is available electronically at https://www.cbp.gov/sites/default/files/assets/documents/2018--Jan/cbp--directive--3340--049a--border--search--electronic--media.pdf, and a copy is attached to this paper as Appendix B. Note that the Directive permits border agents to search only the information that resides on the electronic device, but provides that agents may not intentionally use the device to access information that is stored elsewhere. The Directive also allows agents to demand that the device's owner provide passwords needed to access the information stored on the device.

- If they must be carried, minimize the number carried that contain client information, and minimize the amount of client information stored on them

- Consider carrying a new/clean device for travel (which can perhaps be used to link to information stored in the cloud or on the lawyer's office server)

- If subject to a border inspection of the device, determine whether the inspection is being "requested" or "demanded," and advise the agent that you are a lawyer (providing a bar admission card as back-up) and that the device contains client information

- Know your responsibilities under your state's Rules of Professional Conduct

- **EU's General Data Protection Regulation (GDPR)**. The GDPR becomes effective in the European Union on May 25, 2018. While this paper does not attempt to address the GDPR in detail, a few points are worth noting given their direct impact on franchisors and franchise systems and given that they will surely arise in the context of negotiations between franchisors and franchisees involving EU member countries. GDPR will place stringent restrictions on the collection and use of consumers' personally identifiable information in the EU and strict obligations on collectors and processors of that information. Franchise agreements often ascribe ownership of customer information to the franchisor (even though the information is collected by the franchisee) while making the franchisee responsible for complying with applicable local laws related to the ownership and operation of the unit, which will, in the EU, include compliance with GDPR. It should be expected that the franchisee will argue during the contract negotiations that, since the franchisor owns the customer information, it alone should be the "data collector" under the GDPR and should indemnify the franchisee if the information is incorrectly collected, stored or processed (particularly where the franchisor mandates the computer system used in the units on which the consumers' information is stored). Notwithstanding those contractual provisions, the obligations of the parties under GDPR will be determined by the GDPR itself. Since both the franchisor and franchisee will be collecting, storing and processing customer information, it is likely that they would each be considered a "data collector" under the GDPR and, as such, each have compliance responsibilities. A solid understanding of the GDPR – which will apply extraterritorially with respect to information collected from persons in the EU – will be necessary not only in connection with the ongoing operation of the units, but also in the negotiations of the agreements that precede those operations.

* * * * * * * * * * *

About the Authors

Michael Daigle is a partner in the Chicago law firm of Cheng Cohen, LLC and can be reached at michael.daigle@chengcohen.com.

Sharon Nelson is President of Sensei Enterprises, Inc., a digital forensics, cybersecurity and information technology firm in Fairfax, Virginia. She can be reached at snelson@senseient.com.

Erika Stillabower is Senior Legal Ethics Counsel for the District of Columbia Bar Association, Washington, D.C. She can be reached at estillabower@dcbar.org.

APPENDIX A

(Pennsylvania – Formal Opinion 2011-200)

PENNSYLVANIA BAR ASSOCIATION COMMITTEE ON LEGAL ETHICS AND PROFESSIONAL RESPONSIBILITY

ETHICAL OBLIGATIONS FOR ATTORNEYS USING CLOUD COMPUTING/ SOFTWARE AS A SERVICE WHILE FULFILLING THE DUTIES OF CONFIDENTIALITY AND PRESERVATION OF CLIENT PROPERTY

FORMAL OPINION 2011-200

I. Introduction and Summary

If an attorney uses a Smartphone or an iPhone, or uses web-based electronic mail (e-mail) such as Gmail, Yahoo!, Hotmail or AOL Mail, or uses products such as Google Docs, Microsoft Office 365 or Dropbox, the attorney is using "cloud computing." While there are many technical ways to describe cloud computing, perhaps the best description is that cloud computing is merely "a fancy way of saying stuff's not on your computer."[1]

From a more technical perspective, "cloud computing" encompasses several similar types of services under different names and brands, including: web-based e-mail, online data storage, software-as-a-service ("SaaS"), platform-as-a-service ("PaaS"), infrastructure-as-a-service ("IaaS"), Amazon Elastic Cloud Compute ("Amazon EC2"), and Google Docs.

This opinion places all such software and services under the "cloud computing" label, as each raises essentially the same ethical issues. In particular, the central question posed by "cloud computing" may be summarized as follows:

> May an attorney ethically store confidential client material in "the cloud"?

In response to this question, this Committee concludes:

> Yes. An attorney may ethically allow client confidential material to be stored in "the cloud" provided the attorney takes reasonable care to assure that (1) all such materials remain confidential, and (2) reasonable safeguards are employed to ensure that the data is protected from breaches, data loss and other risks.

****

In recent years, technological advances have occurred that have dramatically changed the way attorneys and law firms store, retrieve and access client information. Many law firms view these

[1] Quinn Norton, "Byte Rights," *Maximum PC*, September 2010, at 12.

technological advances as an opportunity to reduce costs, improve efficiency and provide better client service. Perhaps no area has seen greater changes than "cloud computing," which refers to software and related services that store information on a remote computer, *i.e.,* a computer or server that is not located at the law office's physical location. Rather, the information is stored on another company's server, or many servers, possibly all over the world, and the user's computer becomes just a way of accessing the information.[2]

The advent of "cloud computing," as well as the use of electronic devices such as cell phones that take advantage of cloud services, has raised serious questions concerning the manner in which lawyers and law firms handle client information, and has been the subject of numerous ethical inquiries in Pennsylvania and throughout the country. The American Bar Association Commission on Ethics 20/20 has suggested changes to the Model Rules of Professional Conduct designed to remind lawyers of the need to safeguard client confidentiality when engaging in "cloud computing."

Recent "cloud" data breaches from multiple companies, causing millions of dollars in penalties and consumer redress, have increased concerns about data security for cloud services. The Federal Trade Commission ("FTC") has received complaints that inadequate cloud security is placing consumer data at risk, and it is currently studying the security of "cloud computing" and the efficacy of increased regulation. Moreover, the Federal Bureau of Investigations ("FBI") warned law firms in 2010 that they were being specifically targeted by hackers who have designs on accessing the firms' databases.

This Committee has also considered the client confidentiality implications for electronic document transmission and storage in Formal Opinions 2009-100 ("Metadata") and 2010-200 ("Virtual Law Offices"), and an informal Opinion directly addressing "cloud computing." Because of the importance of "cloud computing" to attorneys – and the potential impact that this technological advance may have on the practice of law – this Committee believes that it is appropriate to issue this Formal Opinion to provide guidance to Pennsylvania attorneys concerning their ethical obligations when utilizing "cloud computing."

This Opinion also includes a section discussing the specific implications of web-based electronic mail (e-mail). With regard to web-based email, *i.e.,* products such as Gmail, AOL Mail, Yahoo! and Hotmail, the Committee concludes that attorneys may use e-mail but that, when circumstances require, attorneys must take additional precautions to assure the confidentiality of client information transmitted electronically.

II. Background

For lawyers, "cloud computing" may be desirable because it can provide costs savings and increased efficiency in handling voluminous data. Better still, cloud service is elastic, and users can have as much or as little of a service as they want at any given time. The service is sold on demand, typically by the minute, hour or other increment. Thus, for example, with "cloud computing," an attorney can simplify document management and control costs.

---

[2] *Id.*

The benefits of using "cloud computing" may include:

- Reduced infrastructure and management;
- Cost identification and effectiveness;
- Improved work production;
- Quick, efficient communication;
- Reduction in routine tasks, enabling staff to elevate work level;
- Constant service;
- Ease of use;
- Mobility;
- Immediate access to updates; and
- Possible enhanced security.

Because "cloud computing" refers to "offsite" storage of client data, much of the control over that data and its security is left with the service provider. Further, data may be stored in other jurisdictions that have different laws and procedures concerning access to or destruction of electronic data. Lawyers using cloud services must therefore be aware of potential risks and take appropriate precautions to prevent compromising client confidentiality, *i.e.*, attorneys must take great care to assure that any data stored offsite remains confidential and not accessible to anyone other than those persons authorized by their firms. They must also assure that the jurisdictions in which the data are physical stored do not have laws or rules that would permit a breach of confidentiality in violation of the Rules of Professional Conduct.

III. Discussion

A. Prior Pennsylvania Opinions

In Formal Opinion 2009-100, this Committee concluded that a transmitting attorney has a duty of reasonable care to remove unwanted metadata from electronic documents before sending them to an adverse or third party. Metadata is hidden information contained in an electronic document that is not ordinarily visible to the reader. The Committee also concluded, *inter alia*, that a receiving lawyer has a duty pursuant to RPC 4.4(b) to notify the transmitting lawyer if an inadvertent metadata disclosure occurs.

Formal Opinion 2010-200 advised that an attorney with a virtual law office "is under the same obligation to maintain client confidentiality as is the attorney in a traditional physical office." Virtual law offices generally are law offices that do not have traditional brick and mortar facilities. Instead, client communications and file access exist entirely online. This Committee also concluded that attorneys practicing in a virtual law office need not take additional precautions beyond those utilized by traditional law offices to ensure confidentiality, because virtual law firms and many brick-and-mortar firms use electronic filing systems and incur the same or similar risks endemic to accessing electronic files remotely.

Informal Opinion 2010-060 on "cloud computing" stated that an attorney may ethically allow client confidential material to be stored in "the cloud" provided the attorney makes reasonable efforts to protect confidential electronic communications and information. Reasonable efforts

discussed include regularly backing up data, installing firewalls, and avoiding inadvertent disclosures.

B. Pennsylvania Rules of Professional Conduct

An attorney using "cloud computing" is under the same obligation to maintain client confidentiality as is the attorney who uses offline documents management. While no Pennsylvania Rule of Profession Conduct specifically addresses "cloud computing," the following rules, *inter alia,* are implicated:

Rule 1.0 ("Terminology");
Rule 1.1 ("Competence");
Rule 1.4 ("Communication");
Rule 1.6 ("Confidentiality of Information");
Rule 1.15 ("Safekeeping Property"); and
Rule 5.3 ("Responsibilities Regarding Nonlawyer Assistants").

Rule 1.1 ("Competence") states:

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

Comment [5] ("Thoroughness and Preparation") of Rule 1.1 provides further guidance about an attorney's obligations to clients that extend beyond legal skills:

> Competent handling of particular matter includes inquiry into and analysis of the factual and legal elements of the problem, and use of methods and procedures meeting the standards of competent practitioners. ...

Competency is affected by the manner in which an attorney chooses to represent his or her client, or, as Comment [5] to Rule 1.1 succinctly puts it, an attorney's "methods and procedures." Part of a lawyer's responsibility of competency is to take reasonable steps to ensure that client data and information is maintained, organized and kept confidential when required. A lawyer has latitude in choosing how or where to store files and use software that may best accomplish these goals. However, it is important that he or she is aware that some methods, like "cloud computing," require suitable measures to protect confidential electronic communications and information. The risk of security breaches and even the complete loss of data in "cloud computing" is magnified because the security of any stored data is with the service provider. For example, in 2011, the syndicated children's show "Zodiac Island" lost an entire season's worth of episodes when a fired employee for the show's data hosting service accessed the show's content without authorization and wiped it out.[3]

---

[3] Eriq Gardner, "Hacker Erased a Season's Worth of 'Zodiac Island'," *Yahoo! TV* (March 31, 2011), available at http://tv.yahoo.com/news/article/tv-news.en.reuters.com/tv-news.en.reuters.com-20110331-us_zodiac

Rule 1.15 ("Safekeeping Property") requires that client property should be "appropriately safeguarded."[4] Client property generally includes files, information and documents, including those existing electronically. Appropriate safeguards will vary depending on the nature and sensitivity of the property. Rule 1.15 provides in relevant part:

> (b) A lawyer shall hold all Rule 1.15 Funds and property separate from the lawyer's own property. Such property shall be identified and appropriately safeguarded.

Rule 1.6 ("Confidentiality of Information") states in relevant part:

> (a) A lawyer shall not reveal information relating to representation of a client unless the client gives informed consent, except for disclosures that are impliedly authorized in order to carry out the representation, and except as stated in paragraphs (b) and (c).
>
> (d) The duty not to reveal information relating to representation of a client continues after the client-lawyer relationship has terminated.

Comment [2] of Rule 1.6 explains the importance and some of the foundation underlying the confidential relationship that lawyers must afford to a client. It is vital for the promotion of trust, justice and social welfare that a client can reasonably believe that his or her personal information or information related to a case is kept private and protected. Comment [2] explains the nature of the confidential attorney-client relationship:

> A fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, the lawyer must not reveal information relating to the representation. See Rule 1.0(e) for the definition of informed consent. This contributes to the trust that is the hallmark of the client-lawyer relationship. The client is thereby encouraged to seek legal assistance and to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter. ...

Also relevant is Rule 1.0(e) defining the requisite "Informed Consent":

> "Informed consent" denotes the consent by a person to a proposed course of conduct after the lawyer has communicated adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct.

Rule 1.4 directs a lawyer to promptly inform the client of any decision with respect to which the client's informed consent is required. While it is not necessary to communicate every minute

---

[4] In previous Opinions, this Committee has noted that the intent of Rule 1.15 does not extend to the entirety of client files, information and documents, including those existing electronically. In light of the expansion of technology as a basis for storing client data, it would appear that the strictures of diligence required of counsel under Rule 1.15 are, at a minimum, analogous to the "cloud."

detail of a client's representation, "adequate information" should be provided to the client so that the client understands the nature of the representation and "material risks" inherent in an attorney's methods. So for example, if an attorney intends to use "cloud computing" to manage a client's confidential information or data, it may be necessary, depending on the scope of representation and the sensitivity of the data involved, to inform the client of the nature of the attorney's use of "cloud computing" and the advantages as well as the risks endemic to online storage and transmission.

Absent a client's informed consent, as stated in Rule 1.6(a), confidential client information cannot be disclosed unless either it is "impliedly authorized" for the representation or enumerated among the limited exceptions in Rule 1.6(b) or Rule 1.6(c).[5] This may mean that a third party vendor, as with "cloud computing," could be "impliedly authorized" to handle client data provided that the information remains confidential, is kept secure, and any disclosure is confined only to necessary personnel. It also means that various safeguards should be in place so that an attorney can be reasonably certain to protect any information that is transmitted, stored, accessed, or otherwise processed through cloud services. Comment [24] to Rule 1.6(a) further clarifies an attorney's duties and obligations:

> When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.

An attorney utilizing "cloud computing" will likely encounter circumstances that require unique considerations to secure client confidentiality. For example, because a server used by a "cloud computing" provider may physically be kept in another country, an attorney must ensure that the data in the server is protected by privacy laws that reasonably mirror those of the United States. Also, there may be situations in which the provider's ability to protect the information is compromised, whether through hacking, internal impropriety, technical failures, bankruptcy, or other circumstances. While some of these situations may also affect attorneys who use offline

---

[5] The exceptions covered in Rule 1.6(b) and (c) are not implicated in "cloud computing." Generally, they cover compliance with Rule 3.3 ("Candor Toward the Tribunal"), the prevention of serious bodily harm, criminal and fraudulent acts, proceedings concerning the lawyer's representation of the client, legal advice sought for Rule compliance, and the sale of a law practice.

storage, an attorney using "cloud computing" services may need to take special steps to satisfy his or her obligation under Rules 1.0, 1.6 and 1.15.[6]

Rule 5.3 ("Responsibilities Regarding Nonlawyer Assistants") states:

> 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:
>
> (1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or
>
> (2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and in either case knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

At its essence, "cloud computing" can be seen as an online form of outsourcing subject to Rule 5.1 and Rule 5.3 governing the supervision of those who are associated with an attorney. Therefore, a lawyer must ensure that tasks are delegated to competent people and organizations. This means that any service provider who handles client information needs to be able to limit authorized access to the data to only necessary personnel, ensure that the information is backed up, reasonably available to the attorney, and reasonably safe from unauthorized intrusion.

It is also important that the vendor understands, embraces, and is obligated to conform to the professional responsibilities required of lawyers, including a specific agreement to comply with all ethical guidelines, as outlined below. Attorneys may also need a written service agreement that can be enforced on the provider to protect the client's interests. In some circumstances, a client may need to be advised of the outsourcing or use of a service provider and the identification of the provider. A lawyer may also need an agreement or written disclosure with the client to outline the nature of the cloud services used, and its impact upon the client's matter.

C. Obligations of Reasonable Care for Pennsylvania/Factors to Consider

[6] Advisable steps for an attorney to take reasonable care to meet his or her obligations for Professional Conduct are outlined below.

In the context of "cloud computing," an attorney must take reasonable care to make sure that the conduct of the cloud computing service provider conforms to the rules to which the attorney himself is subject. Because the operation is outside of an attorney's direct control, some of the steps taken to ensure reasonable care are different from those applicable to traditional information storage.

While the measures necessary to protect confidential information will vary based upon the technology and infrastructure of each office – and this Committee acknowledges that the advances in technology make it difficult, if not impossible to provide specific standards that will apply to every attorney – there are common procedures and safeguards that attorneys should employ.

These various safeguards also apply to traditional law offices. Competency extends beyond protecting client information and confidentiality; it also includes a lawyer's ability to reliably access and provide information relevant to a client's case when needed. This is essential for attorneys regardless of whether data is stored onsite or offsite with a cloud service provider. However, since cloud services are under the provider's control, using "the cloud" to store data electronically could have unwanted consequences, such as interruptions in service or data loss. There are numerous examples of these types of events. Amazon EC2 has experienced outages in the past few years, leaving a portion of users without service for hours at a time. Google has also had multiple service outages, as have other providers. Digital Railroad, a photo archiving service, collapsed financially and simply shut down. These types of risks should alert anyone contemplating using cloud services to select a suitable provider, take reasonable precautions to back up data and ensure its accessibility when the user needs it.

Thus, the standard of reasonable care for "cloud computing" may include:

- Backing up data to allow the firm to restore data that has been lost, corrupted, or accidentally deleted;
- Installing a firewall to limit access to the firm's network;
- Limiting information that is provided to others to what is required, needed, or requested;
- Avoiding inadvertent disclosure of information;
- Verifying the identity of individuals to whom the attorney provides confidential information;
- Refusing to disclose confidential information to unauthorized individuals (including family members and friends) without client permission;
- Protecting electronic records containing confidential data, including backups, by encrypting the confidential data;
- Implementing electronic audit trail procedures to monitor who is accessing the data;

- Creating plans to address security breaches, including the identification of persons to be notified about any known or suspected security breach involving confidential data;

- Ensuring the provider:
    - explicitly agrees that it has no ownership or security interest in the data;
    - has an enforceable obligation to preserve security;
    - will notify the lawyer if requested to produce data to a third party, and provide the lawyer with the ability to respond to the request before the provider produces the requested information;
    - has technology built to withstand a reasonably foreseeable attempt to infiltrate data, including penetration testing;
    - includes in its "Terms of Service" or "Service Level Agreement" an agreement about how confidential client information will be handled;
    - provides the firm with right to audit the provider's security procedures and to obtain copies of any security audits performed;
    - will host the firm's data only within a specified geographic area. If by agreement, the data are hosted outside of the United States, the law firm must determine that the hosting jurisdiction has privacy laws, data security laws, and protections against unlawful search and seizure that are as rigorous as those of the United States and Pennsylvania;
    - provides a method of retrieving data if the lawyer terminates use of the SaaS product, the SaaS vendor goes out of business, or the service otherwise has a break in continuity; and,
    - provides the ability for the law firm to get data "off" of the vendor's or third party data hosting company's servers for the firm's own use or in-house backup offline.

- Investigating the provider's:
    - security measures, policies and recovery methods;
    - system for backing up data;
    - security of data centers and whether the storage is in multiple centers;
    - safeguards against disasters, including different server locations;
    - history, including how long the provider has been in business;
    - funding and stability;
    - policies for data retrieval upon termination of the relationship and any related charges; and,
    - process to comply with data that is subject to a litigation hold.

- Determining whether:
    - data is in non-proprietary format;
    - the Service Level Agreement clearly states that the attorney owns the data;
    - there is a 3rd party audit of security; and,
    - there is an uptime guarantee and whether failure results in service credits.

- Employees of the firm who use the SaaS must receive training on and are required to abide by all end-user security measures, including, but not limited to, the creation of strong passwords and the regular replacement of passwords.

- Protecting the ability to represent the client reliably by ensuring that a copy of digital data is stored onsite.[7]

- Having an alternate way to connect to the internet, since cloud service is accessed through the internet.

The terms and conditions under which the "cloud computing" services are offered, *i.e.,* Service Level Agreements ("SLAs"), may also present obstacles to reasonable care efforts. Most SLAs are essentially "take it or leave it,"[8] and often users, including lawyers, do not read the terms closely or at all. As a result, compliance with ethical mandates can be difficult. However, new competition in the "cloud computing" field is now causing vendors to consider altering terms. This can help attorneys meet their ethical obligations by facilitating an agreement with a vendor that adequately safeguards security and reliability.[9]

Additional responsibilities flow from actual breaches of data. At least forty-five states, including Pennsylvania, currently have data breach notification laws and a federal law is expected. Pennsylvania's notification law, 73 P.S. § 2303 (2011) ("Notification of Breach"), states:

> (a) GENERAL RULE. -- An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. Except as provided in section 4 or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay. For the purpose of this section, a resident of this Commonwealth may be determined to be an individual whose principal mailing address, as reflected in the computerized data which is maintained, stored or managed by the entity, is in this Commonwealth.
>
> (b) ENCRYPTED INFORMATION. -- An entity must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.

---

[7] This is recommended even though many vendors will claim that it is not necessary.

[8] Larger providers can be especially rigid with SLAs, since standardized agreements help providers to reduce costs.

[9] One caveat in an increasing field of vendors is that some upstart providers may not have staying power. Attorneys are well advised to consider the stability of any company that may handle sensitive information and the ramifications for the data in the event of bankruptcy, disruption in service or potential data breaches.

> (c) VENDOR NOTIFICATION. -- A vendor that maintains, stores or manages computerized data on behalf of another entity shall provide notice of any breach of the security system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores or manages the data. The entity shall be responsible for making the determinations and discharging any remaining duties under this act.

A June, 2010, Pew survey highlighted concerns about security for "cloud computing." In the survey, a number of the nearly 900 internet experts surveyed agreed that it "presents security problems and further exposes private information," and some experts even predicted that "the cloud" will eventually have a massive breach from cyber-attacks.[10] Incident response plans should be in place before attorneys move to "the cloud", and the plans need to be reviewed annually. Lawyers may need to consider that at least some data may be too important to risk inclusion in cloud services.

One alternative to increase security measures against data breaches could be "private clouds." Private clouds are not hosted on the Internet, and give users completely internal security and control. Therefore, outsourcing rules do not apply to private clouds. Reasonable care standards still apply, however, as private clouds do not have impenetrable security. Another consideration might be hybrid clouds, which combine standard and private cloud functions.

D. Web-based E-mail

Web-based email ("webmail") is a common way to communicate for individuals and businesses alike. Examples of webmail include AOL Mail, Hotmail, Gmail, and Yahoo! Mail. These services transmit and store e-mails and other files entirely online and, like other forms of "cloud computing," are accessed through an internet browser. While pervasive, webmail carries with it risks that attorneys should be aware of and mitigate in order to stay in compliance with their ethical obligations. As with all other cloud services, reasonable care in transmitting and storing client information through webmail is appropriate.

In 1999, The ABA Standing Commission on Ethics and Professional Responsibility issued Formal Opinion No. 99-413, discussed in further detail above, and concluded that using unencrypted email is permissible. Generally, concerns about e-mail security are increasing, particularly unencrypted e-mail. Whether an attorney's obligations should include the safeguard of encrypting emails is a matter of debate. An article entitled, "Legal Ethics in the Cloud: Avoiding the Storms," explains:

> Respected security professionals for years have compared e-mail to postcards or postcards written in pencil. Encryption is being increasingly required in areas like banking and health care. New laws in Nevada and Massachusetts (which apply to attorneys as well as others) require defined personal information to be encrypted when it is electronically transmitted. As the use of encryption grows in areas like

[10] Janna Quitney Anderson & Lee Rainie, The Future of Cloud Computing. Pew Internet & American Life Project, June 11, 2010, http://www.pewinternet.org/Reports/2010/The-future-of-cloud-computing/Main-Findings.aspx?view=all

> these, it will become difficult for attorneys to demonstrate that confidential client data needs lesser protection.[11]

The article also provides a list of nine potential e-mail risk areas, including: confidentiality, authenticity, integrity, misdirection or forwarding, permanence (wanted e-mail may become lost and unwanted e-mail may remain accessible even if deleted), and malware. The article further provides guidance for protecting e-mail by stating:

> In addition to complying with any legal requirements that apply, the most prudent approach to the ethical duty of protecting confidentiality is to have an express understanding with clients about the nature of communications that will be (and will not be) sent by e-mail and whether or not encryption and other security measures will be utilized.
>
> It has now reached the point (or at least is reaching it) where most attorneys should have encryption available for use in appropriate circumstances.[12]

Compounding the general security concerns for e-mail is that users increasingly access webmail using unsecure or vulnerable methods such as cell phones or laptops with public wireless internet connections. Reasonable precautions are necessary to minimize the risk of unauthorized access to sensitive client information when using these devices and services, possibly including precautions such as encryption and strong password protection in the event of lost or stolen devices, or hacking.

The Committee further notes that this issue was addressed by the District of Columbia Bar in Opinion 281 (Feb. 18, 1998) ("Transmission of Confidential Information by Electronic Mail"), which concluded that, "In most circumstances, transmission of confidential information by unencrypted electronic mail does not per se violate the confidentiality rules of the legal profession. However, individual circumstances may require greater means of security."

The Committee concluded, and this Committee agrees, that the use of unencrypted electronic mail is not, by itself, a violation of the Rules of Professional Conduct, in particular Rule 1.6 ("Confidentiality of Information").

> Thus, we hold that the mere use of electronic communication is not a violation of Rule 1.6 absent special factors. We recognize that as to any confidential communication, the sensitivity of the contents of the communication and/or the circumstances of the transmission may, in specific instances, dictate higher levels of security. Thus, it may be necessary in certain circumstances to use extraordinary means to protect client confidences. To give an obvious example, a lawyer representing an associate in a dispute with the associate's law firm could very easily violate Rule 1.6 by sending a fax concerning the dispute to the law firm's mail room if that message contained client confidential

---

[11] David G. Ries, Esquire, "Legal Ethics in the Cloud: Avoiding the Storms," course handbook, *Cloud Computing 2011: Cut Through the Fluff & Tackle the Critical Stuff* (June 2011) (internal citations omitted).

[12] *Id.*

information. It is reasonable to suppose that employees of the firm, other lawyer employed at the firm, indeed firm management, could very well inadvertently see such a fax and learn of its contents concerning the associate's dispute with the law firm. Thus, what may ordinarily be permissible—the transmission of confidential information by facsimile—may not be permissible in a particularly factual context.

By the same analysis, what may ordinarily be permissible – the use of unencrypted electronic transmission – may not be acceptable in the context of a particularly heightened degree of concern or in a particular set of facts. But with that exception, we find that a lawyer takes reasonable steps to protect his client's confidence when he uses unencrypted electronically transmitted messages.

E. Opinions From Other Ethics Committees

Other Ethics Committees have reached conclusions similar in substance to those in this Opinion. Generally, the consensus is that, while "cloud computing" is permissible, lawyers should proceed with caution because they have an ethical duty to protect sensitive client data. In service to that essential duty, and in order to meet the standard of reasonable care, other Committees have determined that attorneys must (1) include terms in any agreement with the provider that require the provider to preserve the confidentiality and security of the data, and (2) be knowledgeable about how providers will handle the data entrusted to them. Some Committees have also raised ethical concerns regarding confidentiality issues with third-party access or general electronic transmission (*e.g.,* web-based email) and these conclusions are consistent with opinions about emergent emergent "cloud computing" technologies.

The American Bar Association Standing Committee on Ethics and Professional Responsibility has not yet issued a formal opinion on "cloud computing." However, the ABA Commission on Ethics 20/20 Working Group on the Implications of New Technologies, published an "Issues Paper Concerning Client Confidentiality and Lawyers' Use of Technology" (Sept. 20, 2010) and considered some of the concerns and ethical implications of using "the cloud." The Working Group found that potential confidentiality problems involved with "cloud computing" include:

- Storage in countries with less legal protection for data;
- Unclear policies regarding data ownership;
- Failure to adequately back up data;
- Unclear policies for data breach notice;
- Insufficient encryption;
- Unclear data destruction policies;
- Bankruptcy;
- Protocol for a change of cloud providers;
- Disgruntled/dishonest insiders;
- Hackers;
- Technical failures;
- Server crashes;
- Viruses;

- Data corruption;
- Data destruction;
- Business interruption (*e.g.*, weather, accident, terrorism); and,
- Absolute loss (*i.e.*, natural or man-made disasters that destroy everything).

Id. The Working Group also stated, "[f]orms of technology other than 'cloud computing' can produce just as many confidentiality-related concerns, such as when laptops, flash drives, and smart phones are lost or stolen." *Id.* Among the precautions the Commission is considering recommending are:

- Physical protection for devices (*e.g.*, laptops) or methods for remotely deleting data from lost or stolen devices;
- Strong passwords;
- Purging data from replaced devices (*e.g.*, computers, smart phones, and copiers with scanners);
- Safeguards against malware (*e.g.*, virus and spyware protection);
- Firewalls to prevent unauthorized access;
- Frequent backups of data;
- Updating to operating systems with the latest security protections;
- Configuring software and network settings to minimize security risks;
- Encrypting sensitive information;
- Identifying or eliminating metadata from electronic documents; and
- Avoiding public Wi-Fi when transmitting confidential information (*e.g.*, sending an email to a client).

Id. Additionally, the ABA Commission on Ethics 20/20 has drafted a proposal to amend, *inter alia*, Model Rule 1.0 ("Terminology"), Model Rule 1.1 ("Competence"), and Model Rule 1.6 ("Duty of Confidentiality") to account for confidentiality concerns with the use of technology, in particular confidential information stored in an electronic format. Among the proposed amendments (insertions underlined, deletions ~~struck through~~):

> Rule 1.1 ("Competence") Comment [6] ("Maintaining Competence"): "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 technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."
>
> Rule 1.6(c) ("Duty of Confidentiality"): "A lawyer shall make reasonable efforts to prevent the inadvertent disclosure of, or unauthorized access to, information relating to the representation of a client."
>
> Rule 1.6 ("Duty of Confidentiality") Comment [16] ("Acting Competently to Preserve Confidentiality"): "Paragraph (c) requires a ~~A~~ lawyer ~~must~~ to act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons or entities who are participating in the representation of the client or who are subject to the lawyer's supervision or monitoring. See Rules 1.1, 5.1, and 5.3. Factors to

> be considered in determining the reasonableness of the lawyer's efforts include the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, and the cost of employing additional safeguards. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules.

In Formal Opinion No. 99-413 (March 10, 1999), the ABA Standing Committee on Ethics and Professional Responsibility determined that using e-mail for professional correspondence is acceptable. Ultimately, it concluded that unencrypted e-mail poses no greater risks than other communication modes commonly relied upon. As the Committee reasoned, "The risk of unauthorized interception and disclosure exists in every medium of communication, including e-mail. It is not, however, reasonable to require that a mode of communicating information must be avoided simply because interception is technologically possible, especially when unauthorized interception or dissemination of the information is a violation of the law." *Id.*

Also relevant is ABA Formal Opinion 08-451 (August 5, 2008), which concluded that the ABA Model Rules generally allow for outsourcing of legal and non-legal support services if the outsourcing attorney ensures compliance with competency, confidentiality, and supervision. The Committee stated that an attorney has a supervisory obligation to ensure compliance with professional ethics even if the attorney's affiliation with the other lawyer or nonlawyer is indirect. An attorney is therefore obligated to ensure that any service provider complies with confidentiality standards. The Committee advised attorneys to utilize written confidentiality agreements and to verify that the provider does not also work for an adversary.

The Alabama State Bar Office of General Council Disciplinary Commission issued Ethics Opinion 2010-02, concluding that an attorney must exercise reasonable care in storing client files, which includes becoming knowledgeable about a provider's storage and security and ensuring that the provider will abide by a confidentiality agreement. Lawyers should stay on top of emerging technology to ensure security is safeguarded. Attorneys may also need to back up electronic data to protect against technical or physical impairment, and install firewalls and intrusion detection software.

State Bar of Arizona Ethics Opinion 09-04 (Dec. 2009) stated that an attorney should take reasonable precautions to protect the security and confidentiality of data, precautions which are satisfied when data is accessible exclusively through a Secure Sockets Layer ("SSL") encrypted connection and at least one other password was used to protect each document on the system. The Opinion further stated, "It is important that lawyers recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult experts in the field." *Id.* Also, lawyers should ensure reasonable protection through a periodic review of security as new technologies emerge.

The California State Bar Standing Committee on Professional Responsibility and Conduct concluded in its Formal Opinion 2010-179 that an attorney using public wireless connections to conduct research and send e-mails should use precautions, such as personal firewalls and encrypting files and transmissions, or else risk violating his or her confidentiality and competence obligations. Some highly sensitive matters may necessitate discussing the use of

public wireless connections with the client or in the alternative avoiding their use altogether. Appropriately secure personal connections meet a lawyer's professional obligations. Ultimately, the Committee found that attorneys should (1) use technology in conjunction with appropriate measures to protect client confidentiality, (2) tailor such measures to each unique type of technology, and (3) stay abreast of technological advances to ensure those measures remain sufficient.

The Florida Bar Standing Committee on Professional Ethics, in Opinion 06-1 (April 10, 2006), concluded that lawyers may utilize electronic filing provided that attorneys "take reasonable precautions to ensure confidentiality of client information, particularly if the lawyer relies on third parties to convert and store paper documents to electronic records." *Id.*

Illinois State Bar Association Ethics Opinion 10-01 (July 2009) stated that "[a] law firm's use of an off-site network administrator to assist in the operation of its law practice will not violate the Illinois Rules of Professional Conduct regarding the confidentiality of client information if the law firm makes reasonable efforts to ensure the protection of confidential client information."[13]

The Maine Board of Overseers of the Bar Professional Ethics Commission adopted Opinion 194 (June 30, 2008) in which it stated that attorneys may use third-party electronic back-up and transcription services so long as appropriate safeguards are taken, including "reasonable efforts to prevent the disclosure of confidential information," and at minimum an agreement with the vendor that contains "a legally enforceable obligation to maintain the confidentiality of the client data involved." *Id.*

Of note, the Maine Ethics Commission, in a footnote, suggests in Opinion 194 that the federal Health Insurance Portability and Accountability Act ("HIPAA") Privacy and Security Rule 45 C.F.R. Subpart 164.314(a)(2) provide a good medical field example of contract requirements between medical professionals and third party service providers ("business associates") that handle confidential patient information. SLAs that reflect these or similar requirements may be advisable for lawyers who use cloud services.

45 C.F.R. Subpart 164.314(a)(2)(i) states:

> The contract between a covered entity and a business associate must provide that the business associate will:
>
> (A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart;

---

[13] Mark Mathewson, *New ISBA Ethics Opinion Re: Confidentiality and Third-Party Tech Vendors*, Illinois Lawyer Now, July 24, 2009, available at http://www.illinoislawyernow.com/2009/07/24/new-isba-ethics-opinion-re-confidentiality-and-third-party-tech-vendors/

(B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;

(C) Report to the covered entity any security incident of which it becomes aware;

(D) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

Massachusetts Bar Association Ethics Opinion 05-04 (March 3, 2005) addressed ethical concerns surrounding a computer support vendor's access to a firm's computers containing confidential client information. The committee concluded that a lawyer may provide a third-party vendor with access to confidential client information to support and maintain a firm's software. Clients have "impliedly authorized" lawyers to make confidential information accessible to vendors "pursuant to Rule 1.6(a) in order to permit the firm to provide representation to its clients." *Id.* Lawyers must "make reasonable efforts to ensure" a vendor's conduct comports with professional obligations. *Id.*

The State Bar of Nevada Standing Committee on Ethics and Professional Responsibility issued Formal Opinion No. 33 (Feb. 9, 2006) in which it stated, "an attorney may use an outside agency to store confidential information in electronic form, and on hardware located outside an attorney's direct supervision and control, so long as the attorney observed the usual obligations applicable to such arrangements for third party storage services." *Id.* Providers should, as part of the service agreement, safeguard confidentiality and prevent unauthorized access to data. The Committee determined that an attorney does not violate ethical standards by using third-party storage, even if a breach occurs, so long as he or she acts competently and reasonably in protecting information.

The New Jersey State Bar Association Advisory Committee on Professional Ethics issued Opinion 701 (April 2006) in which it concluded that, when using electronic filing systems, attorneys must safeguard client confidentiality by exercising "sound professional judgment" and reasonable care against unauthorized access, employing reasonably available technology. *Id.* Attorneys should obligate outside vendors, through "contract, professional standards, or otherwise," to safeguard confidential information. *Id.* The Committee recognized that Internet service providers often have better security than a firm would, so information is not necessarily safer when it is stored on a firm's local server. The Committee also noted that a strict guarantee of invulnerability is impossible in any method of file maintenance, even in paper document filing, since a burglar could conceivably break into a file room or a thief could steal mail.

The New York State Bar Association Committee on Professional Ethics concluded in Opinion 842 (Sept. 10, 2010) that the reasonable care standard for confidentiality should be maintained for online data storage and a lawyer is required to stay abreast of technology advances to ensure protection. Reasonable care may include: (1) obligating the provider to preserve confidentiality and security and to notify the attorney if served with process to produce client information, (2) making sure the provider has adequate security measures, policies, and recoverability methods,

and (3) guarding against "reasonably foreseeable" data infiltration by using available technology. *Id.*

The North Carolina State Bar Ethics Committee has addressed the issue of "cloud computing" directly, and this Opinion adopts in large part the recommendations of this Committee. Proposed Formal Opinion 6 (April 21, 2011) concluded that "a law firm may use SaaS[14] if reasonable care is taken effectively to minimize the risks to the disclosure of confidential information and to the security of client information and client files." *Id.* The Committee reasoned that North Carolina Rules of Professional Conduct do not require a specific mode of protection for client information or prohibit using vendors who may handle confidential information, but they do require reasonable care in determining the best method of representation while preserving client data integrity. Further, the Committee determined that lawyers "must protect against security weaknesses unique to the Internet, particularly 'end-user' vulnerabilities found in the lawyer's own law office." *Id.*

The Committee's minimum requirements for reasonable care in Proposed Formal Opinion 6 included:[15]

- An agreement on how confidential client information will be handled in keeping with the lawyer's professional responsibilities must be included in the SaaS vendor's Terms of Service or Service Level Agreement, or in a separate agreement that states that the employees at the vendor's data center are agents of the law firm and have a fiduciary responsibility to protect confidential client information and client property;

- The agreement with the vendor must specify that firm's data will be hosted only within a specified geographic area. If by agreement the data is hosted outside of the United States, the law firm must determine that the hosting jurisdiction has privacy laws, data security laws, and protections against unlawful search and seizure that are as rigorous as those of the United States and the state of North Carolina;

- If the lawyer terminates use of the SaaS product, the SaaS vendor goes out of business, or the service otherwise has a break in continuity, the law firm must have a method for retrieving the data, the data must be available in a non-proprietary format that is compatible with other firm software or the firm must have access to the vendor's software or source code, and data hosted by the vendor or third party data hosting company must be destroyed or returned promptly;

---

[14] SaaS, as stated above, stands for Software-as-a-Service and is a type of "cloud computing."

[15] The Committee emphasized that these are minimum requirements, and, because risks constantly evolve, "due diligence and perpetual education as to the security risks of SaaS are required." Consequently, lawyers may need security consultants to assess whether additional measures are necessary.

- The law firm must be able get data "off" the vendor's or third party data hosting company's servers for lawyers' own use or in-house backup offline; and,

- Employees of the firm who use SaaS should receive training on and be required to abide by end-user security measures including, but not limited to, the creation of strong passwords and the regular replacement of passwords.

In Opinion 99-03 (June 21, 1999), the **State Bar Association of North Dakota** Ethics Committee determined that attorneys are permitted to use online data backup services protected by confidential passwords. Two separate confidentiality issues that the Committee identified are, (1) transmission of data over the internet, and (2) the storage of electronic data. The Committee concluded that the transmission of data and the use of online data backup services are permissible provided that lawyers ensure adequate security, including limiting access only to authorized personnel and requiring passwords.

Vermont Bar Association Advisory Ethics Opinion 2003-03 concluded that lawyers can use third-party vendors as consultants for confidential client data-base recovery if the vendor fully understands and embraces the clearly communicated confidentiality rules. Lawyers should determine whether contractors have sufficient safety measures to protect information. A significant breach obligates a lawyer to disclose the breach to the client.

Virginia State Bar Ethics Counsel Legal Ethics Opinion 1818 (Sept. 30, 2005) stated that lawyers using third party technical assistance and support for electronic storage should adhere to Virginia Rule of Professional Conduct 1.6(b)(6)[16], requiring "due care" in selecting the service provider and keeping the information confidential. *Id.*

These opinions have offered compelling rationales for concluding that using vendors for software, service, and information transmission and storage is permissible so long as attorneys meet the existing reasonable care standard under the applicable Rules of Professional Conduct, and are flexible in contemplating the steps that are required for reasonable care as technology changes.

IV. Conclusion

The use of "cloud computing," and electronic devices such as cell phones that take advantage of cloud services, is a growing trend in many industries, including law. Firms may be eager to capitalize on cloud services in an effort to promote mobility, flexibility, organization and efficiency, reduce costs, and enable lawyers to focus more on legal, rather than technical and

---

[16] Virginia Rule of Professional Conduct 1.6(b) states in relevant part:

> To the extent a lawyer reasonably believes necessary, the lawyer may reveal:
>
> (6) information to an outside agency necessary for statistical, bookkeeping, accounting, data processing, printing, or other similar office management purposes, provided the lawyer exercises due care in the selection of the agency, advises the agency that the information must be kept confidential and reasonably believes that the information will be kept confidential.

administrative, issues. However, lawyers must be conscientious about maintaining traditional confidentiality, competence, and supervisory standards.

This Committee concludes that the Pennsylvania Rules of Professional Conduct require attorneys to make reasonable efforts to meet their obligations to ensure client confidentiality, and confirm that any third-party service provider is likewise obligated.

Accordingly, as outlined above, this Committee concludes that, under the Pennsylvania Rules of Professional Conduct an attorney may store confidential material in "the cloud." Because the need to maintain confidentiality is crucial to the attorney-client relationship, attorneys using "cloud" software or services must take appropriate measures to protect confidential electronic communications and information. In addition, attorneys may use email but must, under appropriate circumstances, take additional precautions to assure client confidentiality.

APPENDIX B

(Directive of US Customs and Border Patrol Re Search of Electronic Devices)

U.S. CUSTOMS AND BORDER PROTECTION

CBP DIRECTIVE NO. 3340-049A

DATE: January 4, 2018
ORIGINATING OFFICE: FO:TO
SUPERSEDES: Directive 3340-049
REVIEW DATE: January 2021

SUBJECT: BORDER SEARCH OF ELECTRONIC DEVICES

1 **PURPOSE.** To provide guidance and standard operating procedures for searching, reviewing, retaining, and sharing information contained in computers, tablets, removable media, disks, drives, tapes, mobile phones, cameras, music and other media players, and any other communication, electronic, or digital devices subject to inbound and outbound border searches by U.S. Customs and Border Protection (CBP). These searches are conducted in furtherance of CBP's customs, immigration, law enforcement, and homeland security responsibilities and to ensure compliance with customs, immigration, and other laws that CBP is authorized to enforce and administer.

These searches are part of CBP's longstanding practice and are essential to enforcing the law at the U.S. border and to protecting border security. They help detect evidence relating to terrorism and other national security matters, human and bulk cash smuggling, contraband, and child pornography. They can also reveal information about financial and commercial crimes, such as those relating to copyright, trademark, and export control violations. They can be vital to risk assessments that otherwise may be predicated on limited or no advance information about a given traveler or item, and they can enhance critical information sharing with, and feedback from, elements of the federal government responsible for analyzing terrorist threat information. Finally, searches at the border are often integral to a determination of an individual's intentions upon entry and provide additional information relevant to admissibility under the immigration laws.

2 **POLICY**

2.1 CBP will protect the rights of individuals against unreasonable search and seizure and ensure privacy protections while accomplishing its enforcement mission.

2.2 All CBP Officers, Border Patrol Agents, Air and Marine Agents, Office of Professional Responsibility Agents, and other officials authorized by CBP to perform border searches shall adhere to the policy described in this Directive and any implementing policy memoranda or musters.

2.3 This Directive governs border searches of electronic devices – including any inbound or outbound search pursuant to longstanding border search authority and conducted at the physical border, the functional equivalent of the border, or the extended border, consistent with law and agency policy. For purposes of this Directive, this excludes actions taken to determine if a device functions (e.g., turning a device on and off); or actions taken to determine if physical contraband is concealed within the device itself; or the review of information voluntarily provided by an individual in an electronic format (e.g., when an individual shows an e-ticket on an electronic device to an Officer, or when an alien proffers information to establish admissibility). This Directive does not limit CBP's authority to conduct other lawful searches of electronic devices, such as those performed pursuant to a warrant, consent, or abandonment, or in response to exigent circumstances; it does not limit CBP's ability to record impressions relating to border encounters; it does not restrict the dissemination of information as required by applicable statutes and Executive Orders.

2.4 This Directive does not govern searches of shipments containing commercial quantities of electronic devices (e.g., an importation of hundreds of laptop computers transiting from the factory to the distributor).

2.5 This Directive does not supersede *Restrictions on Importation of Seditious Matter*, Directive 2210-001A. Seditious materials encountered through a border search should continue to be handled pursuant to Directive 2210-001A or any successor thereto.

2.6 This Directive does not supersede *Processing Foreign Diplomatic and Consular Officials*, Directive 3340-032. Diplomatic and consular officials encountered at the border, the functional equivalent of the border (FEB), or extended border should continue to be processed pursuant to Directive 3340-032 or any successor thereto.

2.7 This Directive applies to searches performed by or at the request of CBP. With respect to searches performed by U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) Special Agents exercise concurrently-held border search authority that is covered by ICE's own policy and procedures. When CBP detains, seizes, or retains electronic devices, or copies of information therefrom, and conveys such to ICE for analysis, investigation, and disposition (with appropriate documentation), the conveyance to ICE is not limited by the terms of this Directive, and ICE policy will apply upon receipt by ICE.

3 DEFINITIONS

3.1 Officer. A Customs and Border Protection Officer, Border Patrol Agent, Air and Marine Agent, Office of Professional Responsibility Special Agent, or any other official of CBP authorized to conduct border searches.

3.2 Electronic Device. Any device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players.

3.3 Destruction. For electronic records, destruction is deleting, overwriting, or degaussing in compliance with CBP Information Systems Security Policies and Procedures Handbook, CIS HB 1400-05C.

4 AUTHORITY/REFERENCES. 6 U.S.C. §§ 122, 202, 211; 8 U.S.C. §§ 1225, 1357, and other pertinent provisions of the immigration laws and regulations; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1589a, 1595a(d), and other pertinent provisions of customs laws and regulations; 31 U.S.C. § 5317 and other pertinent provisions relating to monetary instruments; 22 U.S.C. § 401 and other laws relating to exports; Guidelines for Detention and Seizures of Pornographic Materials, Directive 4410-001B; Disclosure of Business Confidential Information to Third Parties, Directive 1450-015; Accountability and Control of Custody Receipt for Detained and Seized Property (CF6051), Directive 5240-005.

The plenary authority of the Federal Government to conduct searches and inspections of persons and merchandise crossing our nation's borders is well-established and extensive; control of the border is a fundamental principle of sovereignty. "[T]he United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity." *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004). "The Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border. Time and again, [the Supreme Court has] stated that 'searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border.'" *Id.* at 152-53 (quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977)). "Routine searches of the persons and effects of entrants [into the United States] are not subject to any requirement of reasonable suspicion, probable cause, or warrant." *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985). Additionally, the authority to conduct border searches extends not only to persons and merchandise entering the United States, but applies equally to those departing the country. *See, e.g., United States v. Boumelhem*, 339 F.3d 414, 422-23 (6th Cir. 2003); *United States v. Odutayo*, 406 F.3d 386, 391-92 (5th Cir. 2005); *United States v. Oriakhi*, 57 F.3d 1290, 1296-97 (4th Cir. 1995); *United States v. Ezeiruaku*, 936 F.2d 136, 143 (3d Cir. 1991); *United States v. Cardona*, 769 F.2d 625, 629 (9th Cir. 1985); *United States v. Udofot*, 711 F.2d 831, 839-40 (8th Cir. 1983).

As a constitutional matter, border search authority is premised in part on a reduced expectation of privacy associated with international travel. *See Flores-Montano*, 541 U.S. at 154 (noting that "the expectation of privacy is less at the border than it is in the interior"). Persons and merchandise encountered by CBP at the international border are not only subject to inspection under U.S. law, they also have been or will be abroad and generally subject to the legal authorities of at least one other sovereign. *See Boumelhem*, 339 F.3d at 423.

In addition to longstanding federal court precedent recognizing the constitutional authority of the U.S. government to conduct border searches, numerous federal statutes and regulations also authorize CBP to inspect and examine all individuals and merchandise entering or departing the United States, including all types of personal property, such as electronic devices. *See, e.g.*, 8 U.S.C. §§ 1225, 1357; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1589a, 1595a; *see also* 19 C.F.R. § 162.6 ("All persons, baggage, and merchandise arriving in the Customs territory of

the United States from places outside thereof are liable to inspection and search by a Customs officer."). These authorities support CBP's enforcement and administration of federal law at the border and facilitate the inspection of merchandise and people to fulfill the immigration, customs, agriculture, and counterterrorism missions of the Department. This includes, among other things, the responsibility to "ensure the interdiction of persons and goods illegally entering or exiting the United States"; "detect, respond to, and interdict terrorists, drug smugglers and traffickers, human smugglers and traffickers, and other persons who may undermine the security of the United States"; "safeguard the borders of the United States to protect against the entry of dangerous goods"; "enforce and administer all immigration laws"; "deter and prevent the illegal entry of terrorists, terrorist weapons, persons, and contraband"; and "conduct inspections at [] ports of entry to safeguard the United States from terrorism and illegal entry of persons." 6 U.S.C. § 211.

CBP must conduct border searches of electronic devices in accordance with statutory and regulatory authorities and applicable judicial precedent. CBP's broad authority to conduct border searches is well-established, and courts have rejected a categorical exception to the border search doctrine for electronic devices. Nevertheless, as a policy matter, this Directive imposes certain requirements, above and beyond prevailing constitutional and legal requirements, to ensure that the authority for border search of electronic devices is exercised judiciously, responsibly, and consistent with the public trust.

5 PROCEDURES

5.1 Border Searches

5.1.1 Border searches may be performed by an Officer or other individual authorized to perform or assist in such searches (e.g., under 19 U.S.C. § 507).

5.1.2 Border searches of electronic devices may include searches of the information stored on the device when it is presented for inspection or during its detention by CBP for an inbound or outbound border inspection. The border search will include an examination of only the information that is resident upon the device and accessible through the device's operating system or through other software, tools, or applications. Officers may not intentionally use the device to access information that is solely stored remotely. To avoid retrieving or accessing information stored remotely and not otherwise present on the device, Officers will either request that the traveler disable connectivity to any network (e.g., by placing the device in airplane mode), or, where warranted by national security, law enforcement, officer safety, or other operational considerations, Officers will themselves disable network connectivity. Officers should also take care to ensure, throughout the course of a border search, that they do not take actions that would make any changes to the contents of the device.

5.1.3 Basic Search. Any border search of an electronic device that is not an advanced search, as described below, may be referred to as a basic search. In the course of a basic search, with or without suspicion, an Officer may examine an electronic device and may review and analyze information encountered at the border, subject to the requirements and limitations provided herein and applicable law.

5.1.4 Advanced Search. An advanced search is any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents. In instances in which there is reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern, and with supervisory approval at the Grade 14 level or higher (or a manager with comparable responsibilities), an Officer may perform an advanced search of an electronic device. Many factors may create reasonable suspicion or constitute a national security concern; examples include the existence of a relevant national security-related lookout in combination with other articulable factors as appropriate, or the presence of an individual on a government-operated and government-vetted terrorist watch list.

5.1.5 Searches of electronic devices will be documented in appropriate CBP systems, and advanced searches should be conducted in the presence of a supervisor. In circumstances where operational considerations prevent a supervisor from remaining present for the entire advanced search, or where supervisory presence is not practicable, the examining Officer shall, as soon as possible, notify the appropriate supervisor about the search and any results thereof.

5.1.6 Searches of electronic devices should be conducted in the presence of the individual whose information is being examined unless there are national security, law enforcement, officer safety, or other operational considerations that make it inappropriate to permit the individual to remain present. Permitting an individual to remain present during a search does not necessarily mean that the individual shall observe the search itself. If permitting an individual to observe the search could reveal law enforcement techniques or potentially compromise other operational considerations, the individual will not be permitted to observe the search itself.

5.2 Review and Handling of Privileged or Other Sensitive Material

5.2.1 Officers encountering information they identify as, or that is asserted to be, protected by the attorney-client privilege or attorney work product doctrine shall adhere to the following procedures.

5.2.1.1 The Officer shall seek clarification, if practicable in writing, from the individual asserting this privilege as to specific files, file types, folders, categories of files, attorney or client names, email addresses, phone numbers, or other particulars that may assist CBP in identifying privileged information.

5.2.1.2 Prior to any border search of files or other materials over which a privilege has been asserted, the Officer will contact the CBP Associate/Assistant Chief Counsel office. In coordination with the CBP Associate/Assistant Chief Counsel office, which will coordinate with the U.S. Attorney's Office as needed, Officers will ensure the segregation of any privileged material from other information examined during a border search to ensure that any privileged material is handled appropriately while also ensuring that CBP accomplishes its critical border security mission. This segregation process will occur through the establishment and employment of a Filter Team composed of legal and operational representatives, or through another appropriate measure with written concurrence of the CBP Associate/Assistant Chief Counsel office.

5.2.1.3 At the completion of the CBP review, unless any materials are identified that indicate an imminent threat to homeland security, copies of materials maintained by CBP and determined to be privileged will be destroyed, except for any copy maintained in coordination with the CBP Associate/Assistant Chief Counsel office solely for purposes of complying with a litigation hold or other requirement of law.

5.2.2 Other possibly sensitive information, such as medical records and work-related information carried by journalists, shall be handled in accordance with any applicable federal law and CBP policy. Questions regarding the review of these materials shall be directed to the CBP Associate/Assistant Chief Counsel office, and this consultation shall be noted in appropriate CBP systems.

5.2.3 Officers encountering business or commercial information in electronic devices shall treat such information as business confidential information and shall protect that information from unauthorized disclosure. Depending on the nature of the information presented, the Trade Secrets Act, the Privacy Act, and other laws, as well as CBP policies, may govern or restrict the handling of the information. Any questions regarding the handling of business or commercial information may be directed to the CBP Associate/Assistant Chief Counsel office or the CBP Privacy Officer, as appropriate.

5.2.4 Information that is determined to be protected by law as privileged or sensitive will only be shared with agencies or entities that have mechanisms in place to protect appropriately such information, and such information will only be shared in accordance with this Directive.

5.3 Review and Handling of Passcode-Protected or Encrypted Information

5.3.1 Travelers are obligated to present electronic devices and the information contained therein in a condition that allows inspection of the device and its contents. If presented with an electronic device containing information that is protected by a passcode or encryption or other security mechanism, an Officer may request the individual's assistance in presenting the electronic device and the information contained therein in a condition that allows inspection of the device and its contents. Passcodes or other means of access may be requested and retained as needed to facilitate the examination of an electronic device or information contained on an electronic device, including information on the device that is accessible through software applications present on the device that is being inspected or has been detained, seized, or retained in accordance with this Directive.

5.3.2 Passcodes and other means of access obtained during the course of a border inspection will only be utilized to facilitate the inspection of devices and information subject to border search, will be deleted or destroyed when no longer needed to facilitate the search of a given device, and may not be utilized to access information that is only stored remotely.

5.3.3 If an Officer is unable to complete an inspection of an electronic device because it is protected by a passcode or encryption, the Officer may, in accordance with section 5.4 below, detain the device pending a determination as to its admissibility, exclusion, or other disposition.

5.3.4 Nothing in this Directive limits CBP's ability, with respect to any device presented in a manner that is not readily accessible for inspection, to seek technical assistance, or to use external equipment or take other reasonable measures, or in consultation with the CBP Associate/Assistant Chief Counsel office to pursue available legal remedies, to render a device in a condition that allows for inspection of the device and its contents.

5.4 Detention and Review in Continuation of Border Search of Information

5.4.1 Detention and Review by CBP

An Officer may detain electronic devices, or copies of information contained therein, for a brief, reasonable period of time to perform a thorough border search. The search may take place on-site or at an off-site location, and is to be completed as expeditiously as possible. Unless extenuating circumstances exist, the detention of devices ordinarily should not exceed five (5) days. Devices must be presented in a manner that allows CBP to inspect their contents. Any device not presented in such a manner may be subject to exclusion, detention, seizure, or other appropriate action or disposition.

5.4.1.1 Approval of and Time Frames for Detention. Supervisory approval is required for detaining electronic devices, or copies of information contained therein, for continuation of a border search after an individual's departure from the port or other location of detention. Port Director; Patrol Agent in Charge; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or other equivalent level manager approval is required to extend any such detention beyond five (5) days. Extensions of detentions exceeding fifteen (15) days must be approved by the Director, Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or other equivalent manager, and may be approved and re-approved in increments of no more than seven (7) days. Approvals for detention and any extension thereof shall be noted in appropriate CBP systems.

5.4.1.2 Destruction. Except as noted in section 5.5 or elsewhere in this Directive, if after reviewing the information pursuant to the time frames discussed in section 5.4, there is no probable cause to seize the device or the information contained therein, any copies of the information held by CBP must be destroyed, and any electronic device must be returned. Upon this determination, the copy of the information will be destroyed as expeditiously as possible, but no later than seven (7) days after such determination unless circumstances require additional time, which must be approved by a supervisor and documented in an appropriate CBP system and which must be no later than twenty-one (21) days after such determination. The destruction shall be noted in appropriate CBP systems.

5.4.1.3 Notification of Border Search. When a border search of information is conducted on an electronic device, the individual subject to search will be notified of the purpose and authority for such search, how the individual may obtain more information on reporting concerns about their search, and how the individual may seek redress from the agency if he or she feels aggrieved by a search. If the Officer or other appropriate CBP official determines that the fact of conducting this search cannot be disclosed to the individual transporting the device without

impairing national security, law enforcement, officer safety, or other operational interests, notification may be withheld.

5.4.1.4 Custody Receipt. If CBP determines it is necessary to detain temporarily an electronic device to continue the search, the Officer detaining the device shall issue a completed Form 6051D to the individual prior to the individual's departure.

5.4.2 Assistance

Officers may request assistance that may be needed to access and search an electronic device and the information stored therein. Except with respect to assistance sought within CBP or from ICE, the following subsections of 5.4.2 govern requests for assistance.

5.4.2.1 Technical Assistance. Officers may sometimes need technical assistance to render a device and its contents in a condition that allows for inspection. For example, Officers may encounter a device or information that is not readily accessible for inspection due to encryption or password protection. Officers may also require translation assistance to inspect information that is in a foreign language. In such situations, Officers may convey electronic devices or copies of information contained therein to seek technical assistance.

5.4.2.2 Subject Matter Assistance – With Reasonable Suspicion or National Security Concern. Officers may encounter information that requires referral to subject matter experts to determine the meaning, context, or value of information contained therein as it relates to the laws enforced or administered by CBP. Therefore, Officers may convey electronic devices or copies of information contained therein for the purpose of obtaining subject matter assistance when there is a national security concern or they have reasonable suspicion of activities in violation of the laws enforced or administered by CBP.

5.4.2.3 Approvals for Seeking Assistance. Requests for assistance require supervisory approval and shall be properly documented and recorded in CBP systems. If an electronic device is to be detained after the individual's departure, the Officer detaining the device shall execute a Form 6051D and provide a copy to the individual prior to the individual's departure. All transfers of the custody of the electronic device will be recorded on the Form 6051D.

5.4.2.4 Electronic devices should be transferred only when necessary to render the requested assistance. Otherwise, a copy of data from the device should be conveyed in lieu of the device in accordance with this Directive.

5.4.2.5 When an electronic device or information contained therein is conveyed for assistance, the individual subject to search will be notified of the conveyance unless the Officer or other appropriate CBP official determines, in consultation with the receiving agency or other entity as appropriate, that notification would impair national security, law enforcement, officer safety, or other operational interests. If CBP seeks assistance for counterterrorism purposes, if a relevant national security-related lookout applies, or if the individual is on a government-operated and government-vetted terrorist watch list, the individual will not be notified of the conveyance, the existence of a relevant national security-related lookout, or his or her presence on a watch list.

When notification is made to the individual, the Officer will annotate the notification in CBP systems and on the Form 6051D.

5.4.3 Responses and Time for Assistance

5.4.3.1 Responses Required. Agencies or entities receiving a request for assistance in conducting a border search are expected to provide such assistance as expeditiously as possible. Where subject matter assistance is requested, responses should include all appropriate findings, observations, and conclusions relating to the laws enforced or administered by CBP.

5.4.3.2 Time for Assistance. Responses from assisting agencies or entities are expected in an expeditious manner so that CBP may complete the border search in a reasonable period of time. Unless otherwise approved by the Director Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager, responses should be received within fifteen (15) days. If the assisting agency or entity is unable to respond in that period of time, the Director Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager may permit extensions in increments of seven (7) days.

5.4.3.3 Revocation of a Request for Assistance. If at any time a CBP supervisor involved in a request for assistance is not satisfied with the assistance provided, the timeliness of assistance, or any other articulable reason, the request for assistance may be revoked, and the CBP supervisor may require the assisting agency or entity to return to CBP all electronic devices provided, and any copies thereof, as expeditiously as possible, except as noted in 5.5.2.3. Any such revocation shall be documented in appropriate CBP systems. When CBP has revoked a request for assistance because of the lack of a timely response, CBP may initiate the request with another agency or entity pursuant to the procedures outlined in this Directive.

5.4.3.4 Destruction. Except as noted in section 5.5.1 below or elsewhere in this Directive, if after reviewing information, probable cause to seize the device or the information from the device does not exist, CBP will retain no copies of the information.

5.5 Retention and Sharing of Information Found in Border Searches

5.5.1 Retention and Sharing of Information Found in Border Searches

5.5.1.1 Retention with Probable Cause. Officers may seize and retain an electronic device, or copies of information from the device, when, based on a review of the electronic device encountered or on other facts and circumstances, they determine there is probable cause to believe that the device, or copy of the contents from the device, contains evidence of a violation of law that CBP is authorized to enforce or administer.

5.5.1.2 Retention of Information in CBP Privacy Act-Compliant Systems. Without probable cause to seize an electronic device or a copy of information contained therein, CBP may retain only information relating to immigration, customs, and other enforcement matters if such retention is consistent with the applicable system of records notice. For example, information

collected in the course of immigration processing for the purposes of present and future admissibility of an alien may be retained in the A-file, Central Index System, TECS, and/or E3 or other systems as may be appropriate and consistent with the policies governing such systems.

5.5.1.3 Sharing Generally. Nothing in this Directive limits the authority of CBP to share copies of information contained in electronic devices (or portions thereof), which are retained in accordance with this Directive, with federal, state, local, and foreign law enforcement agencies to the extent consistent with applicable law and policy.

5.5.1.4 Sharing of Terrorism Information. Nothing in this Directive is intended to limit the sharing of terrorism-related information to the extent the sharing of such information is authorized by statute, Presidential Directive, or DHS policy. Consistent with 6 U.S.C. § 122(d)(2) and other applicable law and policy, CBP, as a component of DHS, will promptly share any terrorism information encountered in the course of a border search with entities of the federal government responsible for analyzing terrorist threat information. In the case of such terrorism information sharing, the entity receiving the information will be responsible for providing CBP with all appropriate findings, observations, and conclusions relating to the laws enforced by CBP. The receiving entity will be responsible for managing retention and disposition of information it receives in accordance with its own legal authorities and responsibilities.

5.5.1.5 Safeguarding Data During Storage and Conveyance. CBP will appropriately safeguard information retained, copied, or seized under this Directive and during conveyance. Appropriate safeguards include keeping materials in locked cabinets or rooms, documenting and tracking copies to ensure appropriate disposition, and other safeguards during conveyance such as password protection or physical protections. Any suspected loss or compromise of information that contains personal data retained, copied, or seized under this Directive must be immediately reported to the CBP Office of Professional Responsibility and to the Port Director; Patrol Agent in Charge; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager.

5.5.1.6 Destruction. Except as noted in this section or elsewhere in this Directive, if after reviewing information, there exists no probable cause to seize the information, CBP will retain no copies of the information.

5.5.2 Retention by Agencies or Entities Providing Technical or Subject Matter Assistance

5.5.2.1 During Assistance. All electronic devices, or copies of information contained therein, provided to an assisting agency or entity may be retained for the period of time needed to provide the requested assistance to CBP or in accordance with section 5.5.2.3 below.

5.5.2.2 Return or Destruction. CBP will request that at the conclusion of the requested assistance, all information be returned to CBP as expeditiously as possible, and that the assisting agency or entity advise CBP in accordance with section 5.4.3 above. In addition, the assisting agency or entity should destroy all copies of the information conveyed unless section 5.5.2.3 below applies. In the event that any electronic devices are conveyed, they must not be destroyed;

they are to be returned to CBP unless seized by an assisting agency based on probable cause or retained per 5.5.2.3.

5.5.2.3 Retention with Independent Authority. If an assisting federal agency elects to continue to retain or seize an electronic device or information contained therein, that agency assumes responsibility for processing the retention or seizure. Copies may be retained by an assisting federal agency only if and to the extent that it has the independent legal authority to do so – for example, when the information relates to terrorism or national security and the assisting agency is authorized by law to receive and analyze such information. In such cases, the retaining agency should advise CBP of its decision to retain information under its own authority.

5.6 Reporting Requirements

5.6.1 The Officer performing the border search of information shall be responsible for completing all after-action reporting requirements. This responsibility includes ensuring the completion of all applicable documentation such as the Form 6051D when appropriate, and creation and/or updating records in CBP systems. Reports are to be created and updated in an accurate, thorough, and timely manner. Reports must include all information related to the search through the final disposition including supervisory approvals and extensions when appropriate.

5.6.2 In instances where an electronic device or copy of information contained therein is forwarded within CBP as noted in section 5.4.1, the receiving Officer is responsible for recording all information related to the search from the point of receipt forward through the final disposition.

5.6.3 Reporting requirements for this Directive are in addition to, and do not replace, any other applicable reporting requirements.

5.7 Management Requirements

5.7.1 The duty supervisor shall ensure that the Officer completes a thorough inspection and that all notification, documentation, and reporting requirements are accomplished.

5.7.2 The appropriate CBP second-line supervisor shall approve and monitor the status of the detention of all electronic devices or copies of information contained therein.

5.7.3 The appropriate CBP second-line supervisor shall approve and monitor the status of the transfer of any electronic device or copies of information contained therein for translation, decryption, or subject matter assistance from another agency or entity.

5.7.4 The Director, Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager shall establish protocols to monitor the proper documentation and recording of searches conducted pursuant to this Directive and the detention, transfer, and final disposition of electronic devices or copies of

information contained therein in order to ensure compliance with the procedures outlined in this Directive.

5.7.5 Officers will ensure, in coordination with field management as appropriate, that upon receipt of any subpoena or other request for testimony or information regarding the border search of an electronic device in any litigation or proceeding, notification is made to the appropriate CBP Associate/Assistant Chief Counsel office.

6 MEASUREMENT. CBP Headquarters will continue to develop and maintain appropriate mechanisms to ensure that statistics regarding border searches of electronic devices, and the results thereof, can be generated from CBP systems using data elements entered by Officers pursuant to this Directive.

7 AUDIT. CBP Management Inspection will develop and periodically administer an auditing mechanism to review whether border searches of electronic devices are being conducted in conformity with this Directive.

8 NO PRIVATE RIGHT CREATED. This Directive is an internal policy statement of U.S. Customs and Border Protection and does not create or confer any rights, privileges, or benefits on any person or party.

9 REVIEW. This Directive shall be reviewed and updated, as necessary, at least every three years.

10 DISCLOSURE. This Directive may be shared with the public.

11 SUPERSEDES. Procedures for Border Search/Examination of Documents, Paper, and Electronic Information (July 5, 2007) and Policy Regarding Border Search of Information (July 16, 2008), to the extent they pertain to electronic devices; CBP Directive No. 3340-049, Border Searches of Electronic Devices Containing Information (August 20, 2009).

Acting Commissioner