IADC COMMITTEE NEWSLETTER

BUSINESS LITIGATION

SEPTEMBER 2015

IN THIS DOUBLE ISSUE

Earlier this year, the United States Supreme Court rendered its decision in North Carolina State Board of Dental Examiners v. Federal Trade Commission, 135 S.Ct. 1101 (2015), holding that a state dental board was not immune from federal antitrust liability under the Parker "state action immunity" doctrine. Future application of the North Carolina Board case creates significant concern not only for state boards and agencies that are comprised of active-market participants but also may signal an erosion of the state action immunity doctrine. Justice Alito, in his dissent, warned the "decision will spawn confusion" recognizing that "whether a state agency is structured in a way that militates against regulatory capture is no easy task…." This article examines the North Carolina State Board decision and some more recent 2015 cases that have attempted to test the limits of state action immunity based upon the Supreme Court's decision.

Also in this month's newsletter, you are careful about locking your office door and setting the alarm, right? To protect your files among other things, right? Are you putting documents in the cloud without taking the same precautions? Matt Cairns explains why the Rules of Professional Conduct make taking such precautions mandatory and offers some Best Practice pointers on how to protect you and your clients should you wish to use the cloud.

Featured Articles

ABOUT THE COMMITTEE

The Business Litigation Committee consists of members involved in business and commercial litigation including business torts, contract and other commercial disputes, e-commerce, antitrust issues, trade secrets and intellectual property, unfair competition and business defamation and disparagement. The Business Litigation Committee helps connect members involved in these areas around the world through networking and referral opportunities; developing and keeping current in the substantive, strategic and procedural aspects of business litigation; and affords members an international forum for sharing current developments and strategies with colleagues. Among the committee's planned activities are newsletters, publications, sponsorship of internal CLEs, and Webinars. Learn more about the Committee at www.iadclaw.org. To contribute a newsletter article, contact:

Martin J. Healy
Vice Chair of Publications
Sedgwick LLP
martin.healy@sedgwicklaw.com

North Carolina State Board of Dental Examiners v. FTC— The Spawning of Confusion

ABOUT THE AUTHORS

Mark Beebe is a Partner in Adams and Reese's Litigation Practice Group, focusing his practice in the areas of antitrust, securities litigation, officers and directors duties, and business and contractual disputes. Mark has been involved in multi-district litigation and class action litigation and appeared before the United States Court of Appeals for the Fifth Circuit, various federal district courts of Louisiana, Mississippi and Pennsylvania, and the state courts of Louisiana, Texas and the District of Columbia. Mark is recognized among the top litigation attorneys by Louisiana Super Lawyers®, Best Lawyers®, Chambers USA and Benchmark Litigation. He is a Fellow of the Litigation Counsel of America. In addition to his litigation practice, Mark serves as the Firm's Business Litigation Team Leader and Liaison Partner--Recruiting, and served formerly as Litigation Practice Group Leader, Associate Liaison and Associate Claims Counsel. Mark also proudly serves as a board member of The Foundation of the International Association of Defense Counsel and was a member of the IADC's legendary Trial Academy Faculty, The Barbourians! He can be reached at mark.beebe@arlaw.com.

Thomas Kimball is a 3L at Loyola University- New Orleans- College of Law. At Loyola, he is an Articles Editor on the Loyola Law Review Board. His case note on the Supreme Court's decision in *Schuette v. BAMN*, 134 S. Ct. 1623 (2014), was selected for publication and will be published in September. Before attending law school, Thomas spent four years working for a practice of psychologists performing various psychological evaluations primarily as defense experts in traumatic brain injury litigation.

Earlier this year, in the matter of *North Carolina State Board of Dental Examiners v. Federal Trade Commission*, 135 S.Ct. 1101 (2015), the United States Supreme Court, in a 6-3 decision, held that a state dental Board was not immune under the *Parker* "state action immunity" doctrine from federal antitrust liability. The Court concluded that the Board was a non-sovereign entity administered and controlled by active market participants and that it was not actively supervised by the state. Consequently, neither the Board nor its members were insulated from liability under the antitrust laws.

The *North Carolina Board* decision is important for state boards and agencies that are comprised of active-market participants. How future courts may apply the *North Carolina Board* decision and its view of the state action immunity doctrine is neither certain nor predictable. Indeed, Justice Alito, in his dissent, warned "there is reason to fear that today's decision will spawn confusion" because "[d]etermining whether a state agency is structured in a way that militates against regulatory capture is no easy task…."[1] The Court advised that in order to protect state agencies and their board members in such circumstances – and ensure that they possess immunity from suit, the state must see that the board or commission operates consistently with state policies through supervision by a politically accountable arm of the state. Absent that supervision, federal antitrust liability—including treble monetary damages—may apply.

Recent challenges to certain government agency decisions suggest that Judge Alito may have been correct. In April, a telemedicine company sued the Texas Medical Board challenging the board's adoption of a code provision that required face-to-face physical examination of patients prior to prescription of any dangerous drug or controlled substance. A month later, the plaintiff obtained a preliminary injunction prohibiting application and implementation of the new rule. *See*, *Teladoc, Inc. et al. v. Texas Medical Board*, *et al.*, 2015 WL 4103658. Similarly, in June, a company offering prepaid legal services brought suit against the North Carolina State Bar objecting to the bar's restrictions on pre-paid legal services arrangements. *See*, *LegalZoom.com, Inc. v. North Carolina State Bar*, *et al*. 2015 WL 3499887.

The *Teladoc* and *LegalZoom* cases support their claims squarely on the *North Carolina State Board* case. The dispute in *North Carolina State Board* related to teeth whitening, a practice that had once been the exclusive province of dentists. In the early 2000s, complaints from dentists began pouring in to the Board about the low prices that non-dentists were charging to perform teeth whitening services.[2] In an effort to respond to the mounting complaints, the Board began an investigation and set "forth to do battle" with non-dentists.[3] The Board did not issue a rule or regulation as a result of the inquiry, which would have been reviewable by the North Carolina Rules Review Commission, whose members are appointed by the legislature. Instead, beginning in 2006, the Board issued numerous cease-and-desist letters to the non-dentist teeth whiteners, warning them that they were engaging in the unlicensed practice of dentistry and to discontinue any such practice.[4] The Board also convinced the North Carolina Board of Cosmetic Art Examiners to warn cosmetologists against performing teeth whitening services and later sent letters to

[1] 135 S. Ct. at 1118.
[2] *Id*. at 1108.
[3] *Id*.
[4] *Id*.

mall operators in an effort to shut down any kiosk teeth whitening services.[5]

In 2010, the Federal Trade Commission ("FTC") charged the Board with violating §5 of the Federal Trade Commission Act alleging that the Board's actions against non-dentist teeth whiteners constituted an anticompetitive and unfair trade practice.[6] Ultimately an ALJ determined that the Board "had unreasonably restrained trade in violation of antitrust law," which was sustained by the FTC on appeal.[7] The FTC then ordered the Board to stop sending the cease-and-desist letters or any other communications aimed at preventing non-dentists from providing teeth whitening services.[8] Additionally, the FTC admonished the Board to issue notices to every provider that it previously sent cease-and-desist letters, advising them of the Board's actual scope of authority.[9] The United States Fourth Circuit Court of Appeals affirmed the FTC in all respects, and the Board sought review from the United States Supreme Court which granted certiorari.[10]

In affirming the Fourth Circuit and FTC decisions, the Court's decision rests primarily on North Carolina's alleged failure to "actively" supervise the board composed primarily of "active market participants." The Board of Dental Examiners is composed of eight Board members, six of which are licensed practicing dentists (elected by other licensed dentists), the seventh member is a licensed practicing dental hygienist (elected by other licensed hygienists), and the eighth is a "consumer" appointed by the Governor.[11] Generally, states are free to impose restrictions on occupations, create shared or exclusive rights to regulate a market, or limit competition in order to achieve their respective public objectives.[12] The Court's decision in *Parker v. Brown* provides immunity from Sherman Act liability for state actions as long as the state acts in its sovereign capacities ("*Parker* immunity").[13]

The Court opined that for non-sovereign actors who are controlled by active market participants to qualify for *Parker* immunity for any anti-competitive policy imposed on the market, it must meet two requirements: (1) the restraint on the market must be "clearly articulated and affirmatively expressed as state policy," and (2) the state must actively supervise the policy.[14] Although the Court expressed doubts as to whether the policy of restraining the trade of non-dentist teeth whiteners was articulated as public policy by the state, it did not need to decide the issue because it was conceded by the parties.[15] Instead, the Court turned to the second requirement: active supervision by the State.

---

[5] *Id.*
[6] *Id.* at 1109.
[7] *Id.*
[8] *Id.*
[9] *Id*.
[10] 717 F.3d 359, 380 (2013); 571 U.S. ---, 134 S. Ct. 1491, 188 L.Ed.2d 375 (2014).
[11] 135 S. Ct. at 1108; N.C. GEN. STAT. ANN. § 90-22.
[12] 135 S. Ct. at 1109-10.
[13] *Id.* at 1110 (citing *Parker v. Brown*, 317 U.S. 341, 350-51 (1943)).
[14] *Id.*
[15] *Id.* at 1110.

The Court reasoned that limits on *Parker* immunity are most essential when, as here, active market participants were delegated regulatory power over other market participants, and therefore, the active market participants should not be free from antitrust accountability.[16] Not only is this a sound precept as a matter of public policy, but the Court iterated that it was an "axiom of federal anti-trust policy."[17] Thus, the Court opined that while *Parker* immunity respects principles of federalism, it does not automatically remove non-sovereign state actors from the overarching axioms of the Supremacy Clause and federal antitrust legislation.[18] This requirement assures that the non-sovereign actors' conduct promotes state policy and not the particular market participants' own interests. [19]

The Court rejected the Board's argument that when a state designates an entity as its agent, it automatically qualifies for *Parker* immunity.[20] The Court also rejected the Board's argument that allowing the FTC order to stand would discourage citizens from serving on state agencies that regulate their own profession.[21] The Court noted that the Board failed to contend that regulating teeth whitening services was supervised by the state "or that it should receive *Parker* immunity on that basis."[22] North Carolina law was free of any language giving the Board the authority to regulate teeth whitening services, the Court found, and even if the Board had the authority, the state failed to supervise the Board's anticompetitive conduct.[23]

In closing, the Court noted that while the inquiry regarding active supervision is "flexible and context-dependent," the Board failed to make any claim that the state actively supervised its conduct regarding teeth whitening services.[24] Thus, there was no supervision system for the Court to analyze.[25] But the Court found that its past precedent required that the state review "the substance of the anticompetitive decision" and this required more than an analysis of the procedures used to carry it out. The state supervisor must have the power to veto or modify particular decisions[26] and must not be an active market participant.[27] The Court declined, however, to provide further specific guidance on how a state agency or its procedures must be structured to ensure active supervision takes place, stating only that it "suffices to note that the inquiry regarding active supervision is flexible and context dependent," and that a state need only adopt mechanisms that provide a "realistic assurance" that such a board or similar entity "promotes state policy, rather than merely the party's individual interests."

---

[16] *Id.* at 1111.
[17] *Id.*
[18] *Id.*
[19] *Id.* at 1112.
[20] *Id.* at 1113-14.
[21] *Id.* at 1115-16.
[22] *Id.* at 1116.
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] *Id.* at 1116-17.
[27] *Id.* at 1117.

Ethical Considerations for Sharing Documents in the Cloud

ABOUT THE AUTHOR

R. Matthew Cairns has been a member of the IADC since 2002. He was President of DRI from 2010-2011. Matt is a shareholder in Gallagher, Callahan & Gartrell in Concord, New Hampshire. He defends individuals and businesses in complex commercial, construction and products liability case in New Hampshire and Vermont. You can follow his ruminations and retweets on Twitter @bigrmc. He can be reached at cairns@gcglaw.com.

It has been just about 1 year since the massive ICloud "hack" where celebrities saw their private and confidential photographs stolen and then made public. Lawyers may not have a stash of salacious photos stored in the cloud, but many of us have equally private and confidential information stored on sites such as DropBox, SugarSync, Box, Microsoft Office 356 and ICloud. Often, your choice of a cloud storage provider will be driven by cost, storage size and ease of use. While important, lawyers more than anyone need to be concerned about security. If you are using cloud storage to collaborate on work, transfer files or make material available to you as you travel, you need to be aware that many states have issued ethics opinions that govern how you use the cloud. This short paper discusses the ethical standards for using the cloud, how you can best use the cloud and also how to let your clients know what you are doing.

Ethical Framework

Rule 1.0(e)

> (e) "Informed consent" denotes the agreement 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 1.1(b)(2)

(b) Legal competence requires at a minimum:

(2) performance of the techniques of practice with skill

ABA Revised Comment 6 to Rule 1.1

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. (emphasis added)

Rule 1.6(a)

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent ….

ABA Revised Comment 16 to Rule 1.6

The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation … 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).

Rule 1.15

(a) Property of clients or third persons which a lawyer is holding in the lawyer's possession in connection with a representation shall … be identified as property of the client, promptly upon receipt, and safeguarded.

Rule 5.3

(b) Each lawyer having direct supervisory authority over the non-lawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer.

***See also* Rule 2.1**

In representing a client, a lawyer shall exercise independent professional judgment [i.e. lawyer cannot hide behind the hired intermediary and ignore how information is stored or transmitted through the cloud]

National Consensus

Nationally, Bar ethics committees that have considered the issue have determined that

lawyers may use cloud computing so long as it is consistent with their ethical duties to protect client data – the lawyer must take reasonable steps to ensure that sensitive client information remains confidential. A table of state ethics decisions collected by the ABA is set forth in Appendix A to this paper.

Lawyers have file drawers full of confidential information in their offices. We are used to protecting that information with locked cabinets, locked doors, and office alarm systems. Using the cloud, however, takes those files and that information out of our immediate control. Outsourcing file maintenance does not relieve a lawyer of his/her duty to perform the techniques with skill. *Rule 1.1(b)(2)*. It might be helpful to consider your cloud provider as another part of your office or your legal team. Rule 5.3 defines a lawyer's responsibilities for non-lawyer assistants: A lawyer shall make reasonable efforts to ensure that the [non-lawyer assistant's] conduct is compatible with the professional obligations of the lawyer. Just like when a lawyer hires an expert, the responsibility rests with him/her to be sure that the intermediary can maintain the confidentiality of the information the lawyer imparts as part of his representation of a client. Lawyers cannot hide behind the intermediary. *Rule 2.1*.

As the ABA Model rules now state:

> 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***…

Rule 1.1, 2012 Revised Comment 6 (emphasis added). Therefore, any competent lawyer must understand and guard against the risks inherent in using cloud computing, just like lawyers of old had to understand and guard against such cutting edge technology as the fax machine. Because technology keeps changing, privacy laws continue to change and hackers become more sophisticated, lawyers need to keep abreast of how those changes affect their use of the cloud and their particular provider.

This knowledge and awareness is fundamental to a lawyer protecting his/her client's confidences while using the cloud. Remember, the file belongs to the client and the lawyer is charged with safekeeping that property for the client. *Rule 1.15*. Rule 1.6 governs confidentiality of client information and communications – protecting the client "file". Simply put, a lawyer shall not reveal information relating to the representation of the client, not just communications with the client. *See ABA Rule 1.6, 2004 Comment 4*. The 2012 ABA revisions added paragraph (c) to Rule 1.6 which reads:

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.

With that change came a revision to Comment 16 which now includes:

> The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation … if the lawyer has made reasonable efforts to prevent the access or disclosure.

The Comment goes on to list a series of factors that should be considered in assessing the reasonable efforts of the lawyer to protect the information:

- 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
- 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)

These revisions to the Rules and comments make clear that the Rules of Professional Responsibility do not set lawyers up for strict liability if there is a hack of your cloud storage site. As one ethics committee observed, "Such a guarantee is impossible, and a lawyer can no more guarantee against unauthorized access to electronic information than he can guarantee that a burglar will not break into his file room, or that someone will not illegally intercept his mail or steal a fax." N.J. Advisory Committee on Professional Ethics Op. No. 701 (electronic filing systems).

What To Do – Best Practices?

There are no guarantees on what steps to protect a lawyer's client's information in the cloud or to vet a vendor will be deemed reasonable. But some Best Practices should be considered.

First, many clients are used to technological collaboration within their organizations. They may even share information with their attorneys in the cloud. This might be seen as an implied authorization to their lawyer to do the same. The client, however, is likely not as sensitive to the ethical issues discussed above as the lawyer is/should be.

Best Practice Tip 1 – get your client's *Informed Consent* before using a cloud service to store or share information related to their case. Rule 1.0(e) defines *Informed Consent* as providing "adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct."

In order to provide information necessary to get Informed Consent about the selected Cloud vendor, the lawyer needs to do some investigation and research.

Best Practice Tip 2 – Research a variety of vendors by asking questions like:

- How does the vendor safeguard the privacy/confidentiality of stored data? Is it encrypted during transmission or just when residing on the server?

- How often does the service back up the user's data? How does the vendor safeguard against natural disaster?

- What is the history of the vendor? Where do they derive their funding? How stable are they financially?

- How does a customer get data "off" the vendor's servers for its own use/backup? If you decide to cancel or change vendors, how will you get your data? Will the data be compatible with other software? (This is very important because at the end of your client relationship, you need to have the information removed from the server and perhaps returned to your client.)

- Does the vendor's Terms of Service or Service Level Agreement address confidentiality and security? If not, would the vendor be willing to sign a confidentiality agreement in keeping with your professional responsibilities?

Once the lawyer selects a vendor, his/her research obligation should not end until the relationship with the client whose information is going onto that vendor's cloud servers ends. The last thing a lawyer wants is to miss a significant development that puts his/her client's information at risk.

Best Practice Tip 3 – keep abreast of what is happening with the vendor you selected. Has there been a recent hack? Have they changed their terms of service? Have the downgraded their security?

Finally, creating a record of the research efforts will protect both the lawyer and his/her client. As discussed above, there are no guarantees, but clear expectations and reasons make for long relationships. A lawyer is partners with his/her client – treat them like a partner on this important decision.

Best Practice Tip 4 – put your intentions in writing along with your rationale and research as part of your effort to obtain *Informed Consent*. This will create a record of what you have done and provide your client the means to provide *Informed Consent*. Draft language for a letter is set forth in Appendix B to this paper.

Conclusion

This paper is not a substitute for your own research into what is required by your state, and you are encouraged to use Appendix A to see if what the specific requirements are in your jurisdiction. That said, the Cloud is here until the next best thing arrives. It is a tool that if used correctly and safely can improve client service as well as how we practice law. If you are going to use the Cloud, be ethical and "Let's Be Careful Out There." Sgt. Esterhaus, Hill Street Blues.

Appendix A – State Ethics Opinions on Cloud Computing

http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html

Jurisdiction	Permitted?	Standard?	Specific Requirements or Recommendations*
ALABAMA Opinion 2010-02	Yes	Reasonable Care	• Know how provider handles storage/security of data. • Reasonably ensure confidentiality agreement is followed. • Stay abreast of best practices regarding data safeguards.
ARIZONA** Opinion 09-04	Yes	Reasonable Care	• "Reasonable security precautions," including password protection, encryption, etc. • Develop or consult someone with competence in online computer security. • Periodically review security measures.
CALIFORNIA Opinion 2010-179	Yes	Reasonable Care	• Evaluate the nature of the technology, available security precautions, and limitations on third-party access. • Consult an expert if lawyer's technology expertise is lacking. • Weigh the sensitivity of the data, the impact of disclosure on the client, the urgency of the situation, and the client's instructions.
CONNECTICUT Informal Opinion 2013-07	Yes	Reasonable Care	• Lawyers ownership and access to the data must not be hindered. • Security policies and processes should segregate the lawyer's data to prevent unauthorized access to the data, including by the cloud service provider.
FLORIDA Opinion 12-3	Yes	Reasonable Care	• Ensure provider has enforceable obligation to preserve confidentiality and security, and will provide notice if served with process. • Investigate provider's security measures • Guard against reasonably foreseeable attempts to infiltrate data.

IOWA Opinion 11-01	Yes	Reasonable Care	• Ensure unfettered access to your data when it is needed, including removing it upon termination of the service. • Determine the degree of protection afforded to the data residing within the cloud service.
MAINE Opinion 207	Yes	Reasonable Care	• Ensure firm technology in general meets professional responsibility constraints. • Review provider's terms of service and/or service level agreements. • Review provider's technology, specifically focusing on security and backup.
MASSACHUSETTS Opinion 12-03	Yes	Reasonable Care	• Review (and periodically revisit) terms of service, restrictions on access to data, data portability, and vendor's security practices. • Follow clients' express instructions regarding use of cloud technology to store or transmit data. • For particularly sensitive client information, obtain client approval before storing/transmitting via the internet.
NEW HAMPSHIRE Opinion #2012-13/4	Yes	Reasonable Care	• Have a basic understanding of technology and stay abreast of changes, including privacy laws and regulations. • Consider obtaining client's informed consent when storing highly confidential information. • Delete data from the cloud and return it to the client at the conclusion of representation or when the file must no longer be preserved. • Make a reasonable effort to ensure cloud providers understand and act in a manner compatible with a lawyer's professional responsibilities.
NEW JERSEY** Opinion 701	Yes	Reasonable Care	• Vendor must have an enforceable obligation to preserve confidentiality and security. • Use available technology to guard against foreseeable attempts to infiltrate data..
NEW YORK Opinion 842	Yes	Reasonable Care	• Vendor must have an enforceable obligation to preserve confidentiality and security, and should notify lawyer if served with process for client data.

			• Use available technology to guard against foreseeable attempts to infiltrate data. • Investigate vendor security practices and periodically review to be sure they remain up-to-date. • Investigate any potential security breaches or lapses by vendor to ensure client data was not compromised.
NEVADA Opinion 33	Yes	Reasonable Care	• Chose a vendor that can be reasonably relied upon to keep client information confidential. • Instruct and require the vendor to keep client information confidential.
NORTH CAROLINA 2011 Formal Ethics Opinion 6	Yes	Reasonable Care	• Review terms and policies, and if necessary re-negotiate, to ensure they're consistent with ethical obligations. • Evaluate vendor's security measures and backup strategy. • Ensure data can be retrieved if vendor shuts down or lawyer wishes to cancel service.
OHIO Informal Advisory Opinion 2013-03	Yes	Reasonable Care	• Competently select appropriate vendor. • Preserve confidentiality and safeguard client property. • Provide reasonable supervision of cloud vendor. • Communicate with the client as appropriate.
OREGON Opinion 2011-188	Yes	Reasonable Care	• Ensure service agreement requires vendor to preserve confidentiality and security. • Require notice in the event that lawyer's data is accessed by a non-authorized party. • Ensure adequate backup. • Re-evaluate precautionary steps periodically in light of advances in technology.
PENNSYLVANIA Opinion 2011-200	Yes	Reasonable Care	• Exercise reasonable care to ensure materials stored in the cloud remain confidential. • Employ reasonable safeguards to protect data from breach, data loss, and other risk.

			• See full opinion for 15 point list of possible safeguards.
VERMONT Opinion 2010-6	Yes	Reasonable Care	• Take reasonable precautions to ensure client data is secure and accessible. • Consider whether certain types of data (e.g. wills) must be retained in original paper format. • Discuss appropriateness of cloud storage with client if data is especially sensitive (e.g. trade secrets).
VIRGINIA Legal Ethics Opinion 1872	Yes	Reasonable Care	• Exercise care in selection of the vendor. • Have a reasonable expectation the vendor will keep data confidential and inaccessible. • Instruct the vendor to preserve the confidentiality of information.
WASHINGTON** Advisory Opinion 2215	Yes	Reasonable Care	• Conduct a due diligence investigation of any potential provider. • Stay abreast of changes in technology. • Review providers security procedures periodically.
WISCONSIN Opinion EF-15-01	Yes	Reasonable Care	• Consider the sensitivity of the data, the impact of the disclosure, the client's circumstances and instructions • Consult an expert if lawyer's technology expertise is lacking. • Understand/know the experience and reputation of the service provider and the terms of their agreement.

* Note that in most opinions, the specific steps or factors listed are intended as non-binding recommendations or suggestions. Best practices may evolve depending on the sensitivity of the data or changes in the technology.

** These opinions address issues which aren't directly labled cloud computing or software as a service, but which share similar technology (e.g.. online backup and file storage).

ABA Cloud Ethics Summary

Jurisdiction	Summary of Opinion
ALABAMA Opinion 2010-02	The Alabama Disciplinary Commission examined cloud computing specifically within the context of storing and producing client files. In that context, the Commission recognized certain benefits of cloud computing, including "the lawyer's increased access to client data" and the possibility that it may also "allow clients greater access to their own files over the internet." That said, the Commission recognized the "confidentiality issues that arise with the use of 'cloud computing,'" specifically that "[c]lient confidences and secrets are no longer under the direct control of the lawyer or his law firm." After reviewing other opinions from both Arizona and Nevada, the Commission eventually concluded "that a lawyer may use "cloud computing" or third-party providers to store client data provided that the attorney exercises reasonable care in doing so." The Commission defined reasonable care as requiring the lawyer to: • Learn how the provider would handle the storage and security of the data; • Reasonably ensure that the provider abides by a confidentiality agreement in handling the data; • Stay abreast of appropriate safeguards that should be employed by both the lawyer and the third-party. In the event that a breach of confidentiality occurs, "the focus of the inquiry will be whether the lawyer acted reasonably in selecting the method of storage and/or the third party provider." Finally, with regard to client files generally, the Commission emphasized that the the format the lawyer uses to store client documents must allow the lawyer "to reproduce the documents in their original paper format," and that the lawyer "must abide by the client's decision in whether to produce the file in its electronic format ... or in its original paper format."
ARIZONA Opinion 09-04	The State Bar of Arizona's Ethics Committee reviewed a query from an Arizona lawyer interested in using "an encrypted online file storage and retrieval system for clients in which all documents are converted to password-protected PDF format and stored in online folders with unique, randomly-generated alpha-numeric names and passwords." In an earlier 2005 opinion, Arizona's Committee had already approved electronic storage of client files where the lawyer or law firm takes "competent and reasonable steps to assure that the client's confidences are not disclosed to third parties through theft or inadvertence." The opinion stated that there were a "panoply of electronic and other measures ... available to assist an attorney" in this regard, and that specific reasonable precautions included "firewalls, password protection schemes, encryption, anti-virus measures, etc." The opinion concluded that the "proposed online client file system appears to meet the requirements" outlined by the rules and the earlier ethics opinion, but did stress that "technology advances may make certain protective

	measures obsolete over time" and therefore "lawyers should periodically review security measures in place to ensure that they still reasonably protect the security and confidentiality of the clients' documents and information."
CALIFORNIA Opinion 2010-179	Recognizing that a technology-by-technology analysis "would likely become obsolete" in a short amount of time, the State Bar of California's Standing Committee on Professional Responsibility and Conduct instead issued an opinion that "sets forth the general analysis that an attorney should undertake when considering use of a particular form of technology." The Committee stated 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," but that the "manner in which an attorney acts to safeguard confidential information is governed by the duty of competence." Examining the issue of competence, the Committee declares that "the duty of competence includes taking appropriate steps to ensure both that secrets and privileged information of a client remain confidential and that the attorney's handling of such information does not result in a waiver of any privileges or protections." The Committee next examines several factors that an attorney should consider before using a given type of technology. These include: • The nature of the technology in relation to more traditional counterparts (i.e. e-mail versus mail). • Reasonable precautions possible to improve the security of a given technology. • Limitations on who can monitor the use of technology and disclose activity. • The lawyer's own level of technological competence, and whether it's necessary to consult with an expert. • Legal ramifications to third parties for intercepting or otherwise interfering with electronic information. • The sensitivity of the data. • Impact of possible disclosure on the client. • Urgency of the situation. • Client instructions. Summing up the opinion, the Committee states that a lawyer must take the appropriate steps to ensure that technology use "does not subject confidential client information to an undue risk of unauthorized disclosure" and must "monitor the efficacy of such steps" on an ongoing basis.
CONNECTICUT Informal Opinion 2013-07	Addressing the question of "whether it is permissible under the Rules of Professional Responsibility for a lawyer to use cloud computing in the practice of law," the Connecticut Bar Association's Professional Ethics Committee found 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." The opinion noted that "Lawyers' remote storage of data is not a new phenomenon; lawyers have been using off-site storage providers for many years, and the issues remain the same whether tangible records are stored in a 'brick-and-mortar' warehouse or intangible data is stored on third party servers." Recognizing the new ABA Model Rule 1.1 comment that lawyers

should "keep abreast of changes in the law and practice, including the benefits and risks associated associated with relevant technology, the Committee concluded that "[i]n order to determine whether use of a particular technology or hiring a particular service provider is consistent or compliant with the lawyer's professional obligations, a lawyer must engage in due diligence."

The Committee discussed several rules to be considered when engaged in this due diligence. They include:

- Rule 1.6(a) - the prohibition against revealing confidential information of a client
- Rule 1.15 - which requires that property of clients and third persons which the lawyer receives should be 'appropriately safeguarded.'
- Rule 5.3 - which addresses a lawyer's duties regarding nonlawyers employed or retained by / associated with a lawyer

This reference to Rule 5.3 seems to be the most important consideration for the Committee. In concluding its opinion, the Committee states that "the lawyer outsourcing cloud computing tasks...must exercise reasonable efforts to select a cloud service provider who...is able to limit authorized access to the data, ensure that the data is preserved...reasonably available to the lawyer, and reasonably safe from unauthorized intrusion."

FLORIDA
Opinion 12-3

The Professional Ethics Committee of the Florida Bar examined the issues surrounding lawyers' use of cloud computing because it "raises ethics concerns of confidentiality, competence, and proper supervision of nonlawyers."

After identifying that confidentiality was the primary concern, the Committee stated that lawyers have an obligation "To maintain as confidential all information that relates to a client's representation, regardless of the source," and that obligation extends to ensuring the "confidentiality of information … maintained by nonlawyers under the lawyer's supervision, including nonlawyers that are third parties used by the lawyer in the provision of legal services." Added to a lawyers obligation to remain current on developments in technology that affect the practice of law, the Committee concludes that lawyers using cloud technology "have an ethical obligation to understand the technology they are using and how it potentially impacts confidentiality of information relating to client matters, so that the lawyers may take appropriate steps to comply with their ethical obligations."

After a review of comparable ethics opinions from other state and local bars, the Committee determined that it agreed with their general finding: cloud computing is permissible "as long as the lawyer adequately addresses the potential risks associated with it."

The Committee goes on to favorably cite the New York State Bar Ethics Opinion 842 with regard to specific due diligence steps, and likewise notes Iowa's Ethics Opinion 11-01 which lists appropriate considerations including using secure passwords, encrypting where possible, and more.

Finally, the Committee adds an additional note that lawyers should "consider whether the lawyer should use the outside service provider or use additional security in specific matters in which the lawyer has proprietary client information or has other particularly sensitive information."

IOWA Opinion 11-01	The Iowa State Bar Association's Ethics Committee evaluated the broad question of whether a lawyer or law firm may use cloud computing or Software as a Service (SaaS). The Committee chose to take a "reasonable and flexible approach to guide a lawyer's use of ever-changing technology" that "places on the lawyer the obligation to perform due diligence to assess the degree of protection that will be needed and to act accordingly." The opinion stressed that lawyers wishing to use SaaS "must ensure that there is unfettered access to the data when it is needed" and that lawyers must also "determine the nature and degree of protection that will be afforded the data while residing elsewhere." In describing these two key requirements, the opinion explores a number of questions that lawyers may need to ask before using such a service, including questions about the legitimacy of the provider, the location where data will be stored, the ability to remove data from the service, and so forth. In terms of data protection, the opinion stresses the need to perform due diligence regarding password protection, access to data, and the ability to encrypt data used in such a service. The opinion concludes by noting that performing due diligence "can be complex and requires specialized knowledge and skill," but allows that lawyers may discharge their ethical duties "by relying on the due diligence services of independent companies, bar associations or other similar organizations or through its own qualified employees."
MAINE Opinion 207	In earlier Opinion 194, the Maine State Bar Association's Professional Ethics Commission conducted a limited review of confidential firm data held electronically and potentially handled by third-party vendors and technicians. Though not directly addressing the cloud, the opinion covered enough common issues that it was previously included in this comparison chart. In January 2013, the Commission revisited the matter to "remove any uncertainty … by squarely and formally addressing the issue" of cloud computing and storage. Overall, the Commission determined that use of such technology was permissible if "safeguards are in place to ensure that the attorney's use of this technology does not result in the violation of any of the attorney's obligations under the various Maine Rules of Professional Conduct." As part of its review, the Commission noted that a number of rules were implicated by the use of cloud technology including 1.1, 1.3, 1.4, 1.6, 1.15, 1.16, 1.17, and 5.3. Yet at the same time, the Commission notes that the "overriding ethical constraints on counsel" have not changed with the evolution of technology; rather, the steps lawyers must take to satisfy those constraints have changed. The Commission notes several internal policies and procedures that lawyers should consider to satisfy their obligations generally under the Rules, including backing up firm data, protecting the firm's network with a firewall, limiting information provided to third parties, and much more. The full list of suggested policies runs to 10 items and draws heavily on Pennsylvania Formal Opinion 2011-200. In addition to these general suggestions regarding firm's technology, the Commission suggests that firm's should also carefully review the terms of

	service or SLA with providers and ensure adequate recognition of the lawyers' professional responsibilities. In addition, lawyers should ensure data will be accessible if the service is terminated and that data will be destroyed at the request of the firm. Finally, lawyers should review the provider's security and backup policies. The Commission goes on to provide some specific guidance regarding how a lawyer may evaluate the provider's technology and terms, including determining ownership of data, the provider's ability to withstand infiltration attempts, and so on. While the opinion includes several lengthy lists of suggested policies and steps to meet ethical obligations, the Commission is clear that the "dynamic nature of the technology make it impossible to list criteria that apply to all situations for all time" and thus adopts the view articulated by the North Carolina Ethics Committee that lawyers must stay educated "on computer technology as it changes and as it is challenged by and reacts to additional indirect factors such as third party hackers or technical failures."
MASSACHUSETTS Opinion 12-03	In this opinion, the Massachusetts Bar Association examined cloud computing in the context of a lawyer who wished to synchronize his files, including confidential client files, between multiple computers using a solution like Google Docs. The MBA recognized that other options were available and drafted the opinion to generally address storage of data in "Internet based storage solutions." Reviewing past opinions that dealt with electronic data and the duty to preserve confidentiality, the MBA Committee concluded that the "the use of an Internet based storage provider to store confidential client information would not violate Massachusetts Rule of Professional Conduct 1.6(a) in ordinary circumstances *as long as* Lawyer undertakes reasonable efforts to ensure that the provider's data privacy policies, practices and procedures are compatible with Lawyer's professional obligations." [Emphasis in the original.] The MBA Committee goes on to list several examples of "reasonable efforts," including examining the provider's written policies and procedures regarding confidential data, ensuring that those terms prohibit unauthorized access to data, ensuring that the lawyer will have reasonable access to and control over the data, examining the provider's security practices (e.g. encryption, password protection) and service history, and periodically revisiting these topics to ensure continued acceptability. The Committee also stresses that a lawyer "remains bound to follow an express instruction from his client that the client's confidential information not be stored or transmitted by means of the Internet" and also that a lawyer "should refrain from storing or transmitting particularly sensitive client information by means of the Internet without first seeking and obtaining the client's express consent to do so." Finally, the Committee concludes by stating that ultimate responsibility for determining whether to use a cloud computing solution resides with the lawyer, who must make the determination "based on the criteria set forth in this opinion, the information that he is reasonably able to obtain regarding the relative security of the various alternatives that are available, and his own sound professional judgment."

NEW HAMPSHIRE
Opinion 2012-13/4

Recognizing that technology has become pervasive in the practice, and that cloud computing in particular "is already a part of many devices" including smartphones and web-based email, New Hampshire sets out to explore the "effect on the lawyer's professional responsibilities."

The opinion focuses on four specific rules: Rule 1.1 Competence, Rule 1.6 Confidentiality, Rule 1.15 Safekeeping Property, and Rule 5.3 Responsibilities Regarding Nonlawyer Assistants. Beginning with Rule 1.1, the opinion notes that recent changes to the comments of ABA Model Rule 1.1 specifically reference the need to "keep abreast of changes in the law and its practice, including the benefits or risks associated with relevant technology." As a result, the opinion stresses that a competent lawyer wishing to use the cloud must understand and guard against the risks inherent to it, and must stay abreast of changes in the technology, privacy laws, and applicable regulations.

On Rule 1.6, the opinion again looks at recent changes to the ABA Model Rules, particularly the factors relating to the reasonableness of a lawyers efforts to keep information confidential. As the relative sensitivity of the information is among those factors, and because not all information is alike, New Hampshire states that "consent of the client to use cloud computing may be necessary" where information is highly sensitive.

On Rule 1.15, the opinion discusses the need to safeguard the client's property--including the client file. Where the contents of that file are stored in the cloud, the lawyer must "take reasonable steps to ensure that the electronic data stored in the cloud is secure and available while representing a client," and that the data can be deleted from the cloud and returned to the client "after representation is concluded or when the lawyer decides to no longer preserve the file."

Finally on Rule 5.3, New Hampshire identifies cloud computing as a form of outsourcing and notes that this requires the lawyer to "make reasonable efforts to ensure that the provider understands and is capable of complying with its obligation to act in a matter compatible with the lawyer's own professional responsibilities." The opinion goes on to stress that this applies as well to any intermediaries the attorney may employee in selecting a provider - e.g. technology consultants or support staff.

While New Hampshire is clear that its opinion addresses a lawyer's obligations and not the technical requirements of the cloud providers, it does conclude with a list of issues which an attorney must address before using the cloud. These include checking the provider's reputation, assessing their security measures, and reviewing the terms of service among other factors.

NEW JERSEY Opinion 701	The opinion from New Jersey's Advisory Committee on Professional Ethics does not focus on cloud-computing specifically, but on the more general topic of storing client files in digital format (e.g. PDF). The committee notes that per an earlier opinion (Opinion 692), certain types of documents are considered "property of the client" and therefore "cannot be preserved...merely by digitizing them in electronic form." The Committee states, however, that "there is nothing in the RPCs that mandates a particular medium of archiving" for other common document types typically included in the client file, such as correspondence, pleadings, memoranda and briefs. Indeed, the Committee states that the lawyer's "paramount consideration is the ability to represent the client competently, and given the advances of technology, a lawyer's ability to discharge those duties may very well be enhanced by having client documents available in electronic form." The Committee goes on to state that putting client documents online through a secure website "has the potential of enhancing communications between lawyer and client, and promotes the values embraced in RPC 1.4." The Committee does acknowledge that electronic document storage presents some risk of unauthorized access, and emphasizes that a lawyer's obligation to maintain client confidentiality "requires that the attorney take reasonable affirmative steps to guard against the risk of inadvertent disclosure." Reasonable care in this case "does not mean that the lawyer absolutely and strictly guarantees that the information will be utterly invulnerable against all unauthorized access." When a lawyer entrusts confidential data to an outside party, however, the "touchstone" for reasonable care requires that "(1) the lawyer has entrusted such documents to an outside provider under circumstances in which there is an enforceable obligation to preserve confidentiality and security, and (2) use is made of available technology to guard against reasonably foreseeable attempts to infiltrate the data."
NEW YORK Opinion 842	The New York State Bar Association's Committee on Professional Ethics examined the question of whether a lawyer could store client's confidential information online without violating professional responsibility rules, and if so, what steps the lawyer should take to ensure the data remains secure. The Committee stresses that a lawyer's duty to maintain client confidentiality includes an affirmative duty to exercise reasonable care in protecting confidential data. This includes exercising reasonable care to prevent inadvertent disclosure by attorney's staff, but does not mean "that the lawyer guarantees that the information is secure from *any* unauthorized access." The Committee notes that "the exercise of reasonable care may differ from one case to the next" based on the sensitivity of the data. Using online data storage to backup (i.e. preserve) client data is deemed ethically permissible where the lawyer has exercised reasonable care "to ensure that the system is secure and that client confidentiality will be maintained." The Committee suggests that this might include ensuring that the vendor has an enforceable obligation to preserve confidentiality and security and will notify the lawyer if served with process requiring production of client data, investigating the vendor's security and backup procedures, and using available technology to guard against reasonably foreseeable attempts to infiltrate it.

	The Committee also writes that lawyers "should periodically reconfirm that the vendor's security measures remain effective in light of advances in technology." If the vendor's methods are insufficient or if the lawyer learns of any breaches effecting the vendor, the lawyer must investigate to be sure his or her clients' data wasn't compromised and if necessary discontinue use of the vendor's service. Lawyers should also stay abreast of general developments in technology insofar as they impact the transmission or storage of electronic files.
NEVADA Opinion 33	The State Bar of Nevada's Standing Committee on Ethics and Professional Responsibility examined whether a lawyer violated their professional responsibility rules "by storing confidential client information and/or communications, without client consent, in an electronic format on a server or other device that is not exclusively in the lawyer's control." The Committee provided that a lawyer "must act competently to safeguard against inadvertent or unauthorized disclosure of confidential client information" by taking "reasonable precautions." The Committee likened the storage of data online to the storage of paper documents in a third-party warehouse, and stated that this was permissible "so long as the attorney observes the usual obligations applicable to such arrangements." This would include, for example, choosing a vendor that "can be reasonably relied upon to maintain the confidentiality" of client data. The opinion also noted that client consent isn't necessary, but that a client "may give informed consent to a means of protection that might otherwise be considered insufficient."
NORTH CAROLINA 2011 Formal Ethics Opinion 6	The North Carolina State Bar's Ethics Committee examined two broad questions in its opinion on cloud computing: first, may a lawyer use cloud computing or software as a service, and second, what measures should a lawyer consider when evaluating a vendor or seeking to reduce the risks associated with the cloud? On the first subject, the Committee's answer is straightforward: yes, lawyers may use the cloud, "provided steps are taken to minimize the risk of inadvertent or unauthorized disclosure of confidential client information and to protect client property." In taking these steps, the lawyer should apply "the same diligence and competency to manag[ing] the risks of SaaS that the lawyer is required to apply when representing clients." On the broader question of the appropriate measures a lawyer should take, the Committee begins by stating hat it "does not set forth specific security

	requirements because mandatory security measures would create a false sense of security in an environment where the risks are continually changing." Rather, the Committee urges lawyers to exercise due diligence and educate themselves regularly about the subject. The Committee does recommend several security measures, however, which includes reviewing applicable terms and policies, and if necessary, negotiating terms regarding how confidential data will be handled. The Committee also suggests that the lawyer have a method of retrieving data if they leave the service or the vendor goes out of business, that the lawyer review the vendor's backup strategy, and finally that the lawyer evaluate the vendor's overall security measures.
OHIO Informal Advisory Opinion 2013-03	The OSBA Informal Advisory Opinion examines a question of "whether [a] law firm may use a third-party vendor to store client data 'in the cloud.'" While acknowledging that previous opinions and rules have traditionally examined "older data storage methods," the Professional Committee writes that the "issues and ethical duties regarding cloud storage are analogous to the ones that apply when lawyers opt to use a vendor to store their paper files offsite rather than in their own offices." Thus, the Committee opts to take a "practical" approach by "applying existing principles to new technological advances while refraining from mandating specific practices." More specifically, the Committee notes that rules about specific security measures would be superseded quickly by technological advances. The Committee addresses the matter in four areas. First, it states that lawyers must "exercise 'due diligence as to the qualifications and reputation of those to whom services are outsourced,' and also as to whether the outside vendor will itself provide the requested services competently and diligently." The Committee specifically suggests a Service Level Agreement and offers some guidance on the types of questions that vendors should be asked. Next, the Committee looks at confidentiality and states that lawyers have a "duty…to maintain the confidentiality of all client data relating to the representation, irrespective of the form of that data, and to carry out that duty with due regard for the form that the data is in." To preserve the confidentiality, a lawyer must exercise competence "(1) in selecting an appropriate vendor, (2) in staying abreast of technology issues that have an impact on client data storage and (3) in considering whether any special circumstances call for extra protection for particularly sensitive client information or for refraining from using the cloud to store such particularly sensitive data." The Committee notes that terms of service that provide or suggest that the vendor has an ownership interest in the data "would violate the duty to keep client property 'identified as such'." Third, the Committee looks at supervision of cloud vendors and states that putting data in the cloud "is almost by definition a service that lawyers will out-source," thus "lawyers who contract with a cloud-storage vendor must make reasonable efforts to ensure that the vendor's conduct is compatible with the lawyer's own professional obligations." On the fourth and final issue, the Committee states that lawyers should use judgment to determine if the circumstances require consultation with the client regarding the use of

	cloud computing. That might arise where the data is of a particularly sensitive nature.
OREGON Opinion 2011-188	The Oregon Committee found that a lawyer "may store client materials on a third-party server as long as Lawyer complies with the duties of competence and confidentiality to reasonably keep the client's information secure within a given situation." That compliance requires "reasonable steps" to ensure that the storage company will secure the client data and preserve its confidentiality. The Committee stated that in some circumstances it may be sufficient for the vendor to be compliant with "industry standards relating to confidentiality and security," but only where those standards "meet the minimum requirements imposed on the Lawyer by the Oregon RPCs. As examples of these requirements, the Committee suggests that lawyers should ensure that "the service agreement requires the vendor to preserve the confidentiality and security of the materials," and that the vendor notify the lawyer if there's any non authorized third-party access to the lawyer's files. The opinion also suggests that lawyers should "investigate how the vendor backs up and stores its data and metadata." Finally, the Committee notes that the reasonableness of the lawyer's protective measures will be judged based on the technology available at the time of disclosure. In other words, the "vendor's protective measures may become less secure or obsolete over time" and therefore the lawyer must reevaluate the measures periodically.
PENNSYLVANIA Opinion 2011-200	The Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility begins its opinion by recognizing that advances in technology, including the cloud, offer opportunities to "reduce costs, improve efficiency and provide better client service." There's also a genuine risk of data breach, particularly given a recent FBI warning that law firms are "being specifically targeted by hackers who have designs on accessing the firms' databases." Noting that an earlier informal opinion (2010-060) had found that a lawyer 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," the Committee dedicates most of this formal opinion to addressing the nature of those "reasonable" efforts. The Committee provides a 15 point list of possible steps a firm "may" take in exercising reasonable care with cloud computing. Several of these steps are routine elements of preserving client confidentiality (e.g. "[r]efusing to disclose confidential information to unauthorized individuals (including family members and friends) without client permission"), but others focus on specific technology issues: • Backing up firm data and maintaining onsite copies; • Using encryption to protect confidential data, including backups; • Developing a plan to address security breaches, including possible notifications to clients; • Evaluating the vendor regarding data ownership, security precautions, the location of data centers, data portability, and more;

	• Providing training to firm staff that will use the cloud tool, including instruction on password best practices; • Having an backup internet connection. Pennsylvania attorneys should review the *full list* published in the opinion. The opinion goes on to stress that "some data may be too important to risk inclusion in cloud services," and also notes that most states have data breach notification laws that lawyers should be familiar with and adhere to in the event that a data breach occurs. The opinion also addresses the question of web-based email, which the Pennsylvania Committee lists as a type of cloud computing. It suggests that attorneys take reasonable precautions "to minimize the risk of unauthorized access to sensitive client information" when using webmail, possibly including specific steps like "encryption and strong password protection"--especially when the data is of a particularly sensitive nature.
VERMONT Opinion 2010-6	The Vermont Bar Association's Professional Responsibility Section addressed the "propriety of use by attorneys and law firms of Software as a Service ("SaaS") which is also known as Cloud Computing." In its analysis, it looked at storing client data in the cloud, possible data types that should not be stored online, as well as specific Cloud uses such as web-based email, calendaring, and remote document synchronization. A significant portion of the Section's analysis is focused on reviewing other recent cloud computing ethics opinions from other jurisdictions, including North Carolina, California, and New York. Drawing upon these opinions and its own analysis, the Section "agrees with the consensus view" that lawyers are obligated to provide "competent representation" while "maintaining confidentiality of client information, and protecting client property in their possession." In choosing whether to use new technologies, including the cloud, lawyers must exercise their due diligence. The Section provides a list of steps a lawyer may take, though it stresses that is not providing a formal "checklist of factors a lawyer must examine." This loose list of factors includes reviewing the vendor's security, checking for limitations on access to or protection of data, reviewing terms of service, examining vendor confidentiality policies, weighing the sensitivity of data placed in the cloud, reviewing other regulatory obligations, and requiring notice if a third party accesses or requests access to data. In addition to those factors, the Section adds that a lawyer may consider giving notice to the client when using the cloud to store client's data, and may want to look to expert third parties to review the vendor's security and access systems. Finally, the Section stresses that lawyers should take "reasonable measures to stay apprised of current developments regarding SaaS systems and the benefits and risks they present."
VIRGINIA Legal Ethics Opinion 1872	Virginia Legal Ethics Opinion 1872 examines a variety of ethical issues associated with virtual law offices, including the use of cloud computing. This summary focuses specifically on the elements of the opinion dealing with cloud computing, but readers are encouraged to view the full text of the opinion to understand the context.

	The opinion begins by stating that lawyers "must always act competently to protect the confidentiality of client information, regardless of how that information is stored/transmitted," but notes that the task may be more challenging when the information is being "transmitted and/or stored electronically through third-party software and storage providers." The opinion notes that the duty is not to "absolutely guarantee that a brief of confidentiality cannot occur," only to "act with reasonable care to protect information relating to the representation of a client." Specifically, lawyers are instructed to carefully select vendors, instruct the vendor to preserve confidentiality, and to have a reasonable expectation that the vendor will in fact keep data confidential and inaccessible. To do that, lawyers must "examine the third party provider's use of technology and terms of service" and, if they're unable to make an assessment on their own, "consult with someone qualified to make that determination."
WASHINGTON Advisory Opinion 2215	In Advisory Opinion 2215, the Washington State Bar Association's Rules of Professional Conduct Committee examined lawyers' ethical obligations relating "to the use of online data storage managed by third party vendors to store confidential client documents." The opinion focused specifically on data storage rather than the broader category of cloud computing, but addressed many issues common to both platforms. In its analysis, the Committee noted that such an arrangement places "confidential client information … outside of the direct control of the lawyer" and thus raises some concern. In particular, the Committee notes lawyers' obligations to preserve confidentiality under RPC 1.6 and to protect client property under RPC 1.15A. Acknowledging that specific guidelines regarding security are impossible "because the technology is changing too rapidly," and also noting that it's "impractical to expect every lawyer who uses such services to be able to understand the technology sufficiently in order to evaluate a particular service provider's systems," the Committee nonetheless suggested that a lawyer must conduct a due diligence investigation of the provider and "cannot rely on lack of technological sophistication to excuse the failure to do so." The Committee offered several steps to conduct such a due diligence investigation, including familiarizing oneself with the risks of online data storage, evaluating the provider's history, comparing terms with other providers, ensuring notice of any non-authorized access to lawyer's data, and generally ensuring that data is secured and backed up. Finally, the Committee also noted that under RPC 1.1 a lawyer has a duty to stay abreast of changes in the law and its practice, and that necessarily includes staying informed about the risks associated with the technology the lawyer employs in his or her practice. As technology evolves, the lawyer must also "monitor and regularly review the security measures of the provider" he or she uses for online data storage.
WISCONSIN Opinion EF-15-01	Wisconsin Formal Ethics Opinion EF-15-01 (Ethical Obligations of Attorneys Using Cloud Computing), issued by the State Bar of Wisconsin's Professional Ethics Committee, notes that increased lawyer accessibility to cloud-based platforms and services comes with a direct loss of control over client

information but that lawyers can use cloud computing services if the lawyer uses reasonable efforts to adequately address the potential risks associated with it. "To be reasonable," the opinion states, "the lawyer's efforts must be commensurate with the risks presented." The opinion acknowledges that lawyers cannot guard against every conceivable danger when using cloud-based services, but lists numerous factors to consider when assessing the risk of using cloud-based services in their practices:

- The information's sensitivity
- The client's instructions and circumstances
- The possible effect that inadvertent disclosure or unauthorized interception could pose to a client or third party
- The attorney's ability to assess the technology's level of security
- The likelihood of disclosure if additional safeguards are not employed
- The cost of employing additional safeguards
- The difficulty of implementing the safeguards
- The extent to which the safeguards adversely affect the lawyer's ability to represent clients
- The need for increased accessibility and the urgency of the situation
- The experience and reputation of the service provider
- The terms of the agreement with the service provider
- The legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality

The opinion also states that in determining what efforts are reasonable to address the cloud-computing risk, lawyers should understand a number of computer security concepts:

- Firewalls
- Virus and spyware programs
- Operating system updates
- Strong passwords and multifactor identification
- Encryption for stored information
- Dangers of using public wi-fi
- Risks of file-sharing sites
- Options for using a virtual private network (VPN)
- The importance of regularly backing up data

Appendix B – Sample Letter to Client About Use of Cloud

During the course of our representation of you, members of this office and retained experts/consultants may find it appropriate to use third party Internet based data storage and sharing services (the "Cloud") such as _____ to store confidential client information and attorney work-product. We may also choose to use those services to synchronize data over the internet.

In in connection with the use of these or any other services, and in compliance with [insert your state's ethics opinion], this office has undertaken reasonable efforts to confirm that the services will adequately protect confidential client information under Rule 1.6 which provides:

> (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).
>
> (b) A lawyer may reveal such information to the extent the lawyer reasonably believes necessary:
>
> (1) to prevent reasonably certain death or substantial bodily harm or to prevent the client from committing a criminal act that the lawyer believes is likely to result in substantial injury to the financial interest or property of another; or
>
> (2) to secure legal advice about the lawyer's compliance with these Rules; or
>
> (3) to establish a claim or defense on behalf of the lawyer in controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client; or
>
> (4) to comply with other law or a court order.

To that end, we have:

- Reviewed the operational history, terms of use, policies, practices and procedures of _____ with regard to data privacy and the handling of confidential information (including back-ups, encryption and

password protection) to prohibit unauthorized access to data stored on the services' system; and

- Ensured that we and you will have access to and control over the data stored on the service in the event our relationship with the service is interrupted.

We will also periodically review the service for any changes to its terms of use, policies, practices and procedures.

Therefore, we would like your consent to, if appropriate, use third party Internet based data storage and sharing service _____ to store confidential client information and attorney work-product, and if necessary use those services to synchronize data over the internet.

If you have any questions about this or would like more information about research on _____ we have undertaken, you should, of course contact us.

If this is acceptable to you, please sign where indicated below.

Past Committee Newsletters

Visit the Committee's newsletter archive online at www.iadclaw.org to read other articles published by the Committee. Prior articles include:

JULY 2015
The Friendly Quebec Class Action Landscape
Éric Azran and Patrick Desalliers

JUNE 2015
Down but Not Out: Bankruptcy's Effect on Diversity of Citizenship
Steven A. Meckler and Christian H. Staples

Making the Right Impression: 15 Proven Strategies for Keeping a Judge Happy
J. Walter Sinclair

APRIL 2015
Consent Provisions in Lease Agreements: Must the Lessor Act Reasonably?
Kristin Olson and Scott Brooksby

FEBRUARY 2015
The Singapore International Commercial Court ("SICC"): Hybrid litigation and arbitration?
Tan Chuan Thye

Location, Location, Location: Drafting Enforceable Forum-Selection Clauses under Atlantic Marine
Diane Fleming Averell and Pamela R. Kaplan

JANUARY 2015
The Waiting Game: Litigators Must Wait a Little While Longer For CMS Guidance on Medicare Set Asides
Ricky M. Guerra and Alexander D. MacMullan

South Carolina Decides Case of First Impression in Recurring Area of "Promoter Liability"
Val H. Stieglitz

NOVEMBER 2014
The Scourge of Fraudulent Transfer Litigation
Creighton "Chip" Magid and Chimera Thompson

OCTOBER 2014
Design and Construction Companies Take Notice: The Statute of Repose Has Teeth in Pennsylvania Asbestos Litigation
Maria Karos and S. Vance Wittie

AUGUST 2014
Be the "Less Bad"
Margaret Fonshell Ward

JULY 2014
Supreme Court Affirms Vitality of Lanham Act Unfair Competition Claims in Two Separate Cases
Gerald P. Schneeweis and Timothy Toohey

JUNE 2014
Termination of Canadian Distribution Agreements and Contractual Duties of Good Faith
Steven Rosenhek