Connecticut Bar Association

Professional Ethics Committee

30 Bank Street
PO Box 350
New Britain
CT 06050-0350
06051 for 30 Bank Street
P: (860) 223-4400
F: (860) 223-4488

Approved June 19, 2013

Informal Opinion 2013-07
Cloud Computing

The question addressed in this Opinion is whether it is permissible under the Rules of Professional Responsibility for a lawyer to use cloud computing in the practice of law.

Technological change tends to outpace the law. There is a great deal being written about cloud computing every day. This opinion is a starting point for issues raised by a lawyer's use of cloud computing, but the field will continue to develop and due diligence will require a lawyer to keep pace with emerging standards. For the purpose of this opinion, cloud computing includes the storage, transmission, and processing of data (client information) using shared computer facilities owned or leased by a third party service provider. The facilities and services are typically accessed over the internet by means of different networked devices including computers, tablets, laptops, smart phones, and other devices.[1]

In a familiar model, a user may be provided with applications referred to as Software as Service ("SAAS"), that operate on a cloud infrastructure which may be located at remotes sites in and outside of Connecticut, including foreign countries. The cloud service provider owns or leases the data processing equipment and the information technology and also manages the system. In the modality which this Opinion addresses – called public cloud computing – the use of the online computer resources is shared with other members of the public.[2] In related activities, a user may entrust data for online storage only (i.e., by using such vendors as are located at mozy.com and cabonite.com) and for online transmission (email via vendors such as aol.com, yahoo.com, gmail.com, outlook.com, etc.). Cloud computing has been the subject of a great deal of commentary; attempts to describe cloud computing have been problematic because cloud computing is not a single kind of system, but instead spans a spectrum of underlying technologies, configuration possibilities, service models, and deployment models.[3]

Cloud computing can provide significant economy and technological benefit for the user compared to what is financially available through the ownership or lease of equipment, direct license of software, and hired information technology personnel. The cloud service providers tend to use a "pay-as-you-go" billing format that offers enormous advantages for users with

[1] See National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication #800-145 (September 2011).
[2] Deployment models include private cloud, community cloud, public cloud, and hybrid cloud infrastructures. NIST #800-145.
[3] National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication #800-146 (May 2012) and Special Publication #800-144 (December 2011).

limited or irregular cash flow. With cloud computing, a user has the option to create a virtual office with only limited ownership of data processing, transmission, and data storage equipment.

The ultimate responsibility for insuring the privacy and security of the data resides with the user purchasing the cloud services. While much of the physical, technical, and administrative safeguards are handled by the cloud service provider, the user will still retain responsibility for a significant portion of these safeguards.

Ordinarily the cloud service provider offers an agreement to a user, which may be called Service Level Agreement ("SLA") or Terms of Service. The terms of such agreements can vary amongst the different service providers, and different terms have different impacts on a lawyer's obligations under applicable law and Rules of Professional Responsibility; this Opinion is limited to discussion of the Connecticut-licensed lawyer's obligations under the Connecticut Rules of Professional Responsibility when using cloud computing.

The privilege of practicing law comes with professional obligations and those obligations extend to the use of technology. Rule 1.1 Official Commentary (effective [month, year]) expressly provides that in order "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 . . . . " 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. If a lawyer is unable to meet these obligations when using a given type of technology or service provider, the lawyer should not use the technology or the service provider. In order to determine whether use of a particular technology or hiring a certain particular service provider is consistent or compliant with the lawyer's professional obligations, a lawyer must engage in due diligence.

Lawyers have professional obligations which include the duty to preserve client information (Rules 1.6 and Rule 1.15) as well as the duty to comply with and respond to legitimate inquiry from disciplinary authorities. Rule 1.15(k) and Practice Book §2-27(c). The issue of how a lawyer stores and processes business records affects the lawyer's ability to discharge these duties. Modern technologies allow for data to be processed, transmitted, and stored some place other than a lawyer's workplace. 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.

Rule 1.6 of the Rules of Professional Conduct governs the confidentiality of client information. In relevant part, Rule 1.6(a) provides that "a lawyer shall not reveal confidential information relating to the representation of a client unless the client consents after consultation . . . . " The duty of confidentiality imposed by Rule 1.6(e) (effective January 1, 2014) requires a lawyer to avoid using means or methods of holding and delivering data that present an unreasonable risk of unintended disclosure to and access by unauthorized third parties. The duty of confidentiality described in Rule 1.6 is rigid but tempered by the recognition that even when a lawyer acts competently to preserve the confidentiality of the data, reasonable safeguards some times fail:

> 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 subsection (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.

Rule 1.6, Official Commentary (effective January 1, 2014).

This Committee previously addressed issues of client confidentiality presented by a lawyer's use of the Internet and remote access capabilities in Informal Opinion 99-52, in which the Committee concluded that a lawyer's use of unencrypted internet email to engage in communication with a client did not violate Rule 1.6(a) in ordinary circumstances. However:

> [I]f circumstances exist which would place a lawyer on notice that there is a greater than ordinary risk of interception or unauthorized disclosure (such as an email "mailbox" which is accessible to persons other than the intended recipient), regardless of the relative sophistication of the email recipient, use of email to transmit confidential information without the express authorization and consent of the client would be unwise and unethical.
>
> In a similar fashion, where the information sought to be communicated is of an extraordinary sensitive or highly confidential nature, such that any unauthorized disclosure could cause serious injury to the interests of the client, the lawyer should choose a means of communication that provides a level of security proportional to the heightened need to avoid any threat of disclosure of the information. Because of this, the consent of the client should be obtained before transmitting any email containing information of an extraordinarily sensitive or highly confidential nature, just as a wise and prudent lawyer would obtain the consent of the client before communicating significant, consequential, and extremely sensitive privileged matters through telephone lines, fax machines, or even regular mail.

Informal Opinion 99-52.

While the specific technology examined by the Committee in 1999 (for Informal Opinion 99-52) might now be obsolete, the need for a lawyer to thoughtfully and thoroughly evaluate the risks presented by the use of current technology remains as vital as ever. The Rules permit a lawyer to use the Internet to transmit, store and process data using shared computer facilities from the reasonably reliable cloud service provider as long as the lawyer undertakes reasonable efforts to prevent unauthorized access to or disclosure of such data. As considered by this Committee in 1999, the lawyer's efforts must be commensurate with the risk presented. The lawyer should be satisfied that the cloud service provider's (1) transmission, storage and possession of the data does not diminish the lawyer's ownership of and unfettered accessibility to the data, and (2) security policies and mechanisms to segregate the lawyer's data and prevent unauthorized access to the data by others including the cloud service provider.[4]

The lawyer's obligations regarding the security for such data are not independent from but consistent with Rule 1.15, which requires that property of clients and third persons which the lawyer receives should be "appropriately safeguarded." Client property in the context of Rule 1.15 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 property of clients and third persons that is in a lawyer's possession in connection with a representation separate from the lawyer's own property. . . . Other property shall be identified as such and appropriately safeguarded.

Further, the lawyer using cloud computing must ensure the service provider's conduct is compatible with the professional obligations of the lawyer. Rule 5.3 addresses the lawyer's responsibilities regarding nonlawyer assistants and states:

> With respect to a nonlawyer employed or retained by or associated with a lawyer:
> (1) 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.
> (2) 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
> (3) 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: (A) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or (B) 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

[4] Many service providers offer different levels of service. Free services provide fewer security and other protections than do paid services. As of the date of this Opinion, the "pro" versions of software and web services generally provide greater protections.

time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

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

In summary, the use of cloud computing is a growing trend in many industries and professions, including law. Lawyers may use cloud services in their practice to promote mobility, flexibility, organization and efficiency. However, lawyers must be conscientious to comply with the duties imposed by the Rules to knowledgeably and competently maintain confidentiality and supervisory standards. The Rules require that lawyers make reasonable efforts to meet their obligations to preserve the confidentiality of client information and to confirm that any third-party service provider is likewise obligated.[5]

THE COMMITTEE ON PROFESSIONAL ETHICS

By_____
John R. Logan, Chair

[5] As of the date of this Opinion, other states have uniformly concluded that cloud computing, as generally defined, is ethically permissible as long as reasonable care is used by the lawyer to ensure access to and the security of the information stored. E.g., AL Ethics Op. 2010-2; AZ Bar Ethics Op. 09-04 (2009); CA Ethics Op. 2010-179; FL Bar Ethics Op. 06-1 (2006); IA Ethics O. 11-01 (2011); IL Bar Ethics Op. 10-01 (2009); MA Bar Ethics Op. 12-03 (2012); ME Bar Ethics Op. 194 (2008); NH Bar Ethics Op. 2012-13/4 (2012); NC Bar Ethics Op. 6 (2011); ND Bar Ethics Op. 99-03; NJ Bar Ethics Op. 107 (2006); NV Bar Ethics Op. 33 (2006); NY State Bar Ethics Op. 842 (2010); OR Bar Ethics Op. 2011-188 (2011); PA Bar Ethics Op. 2011-200 (2011); VA Ethics Op. 1818 (2005); VT Ethics Op. 2003-03 (2003).