

An Update on Governing Cloud Computing

By Will Hornsby and Joseph Duffy

December 2011

Cloud computing raises questions of practice management, as new ethical directions emerge. Lawyers have a duty to protect and secure electronic files, even if not trained in the world of technology.

Cloud computing may be adding another layer to our practice management responsibilities, as direction for our ethics obligations start to emerge. Cloud computing is defined in various ways, but for the purpose of this article it is best considered the use of a network of remote servers hosted on the Internet to store, manage and process data, rather than on a local server.

Examples of cloud computing include Gmail, Google Docs, iCloud, and Dropbox. Emails, pictures and documents are stored on Internet-based servers located around the world and are accessible via a login page from any computer connected to the Internet. Data is not only stored on the computer in a lawyer's office, but also remotely, in the hands of a third party. Cloud services are a convenient and attractive method for communication and data storage; they are often free, simple, fast, and accessible from anywhere in the world. Unfortunately, those conveniences raise issues of privacy and client confidentiality that lawyers must scrutinize before deciding to use them.

The central concern when considering communications in the cloud involves our obligation to maintain the client information confidential. ABA Model Rule 1.6 governs the confidentiality of information relating to the representation of clients. Comment 16 of that rule charges lawyers with the responsibility to "competently safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure." In the pre-digital age the rule required a lawyer to take reasonable measures such as locking the office door or file cabinets at the end of the day. Today lawyers have a duty to protect and secure electronic files, even if the lawyer is not trained in the world of technology.

Our obligations are beginning to be defined through state ethics opinions, while, at the same time, the ABA is weighing in with thoughts about amendments to the Model Rules.

State Opinions

Some states have now addressed responsibilities when engaged in cloud computing. For the most part, the ethics opinions are consistent, although some have a higher degree of scrutiny.

In Opinion 701, the New Jersey State Advisory Committee on Professional Ethics emphasized the lawyer's responsibilities to take affirmative steps to guard against inadvertent disclosures and exercise "reasonable care" against unauthorized access when using cloud services. The committee found

reasonable care to constitute an enforceable obligation on the third party to maintain confidentiality and security, as well as the use of technology to safeguard against conceivable attempts to gain unauthorized access, just as a security system or file cabinet locks were necessary in the pre-digital age. The Committee noted that an absolute guarantee against unauthorized access is impossible, and as with paper records a third party may use illegal means to access the files. The committee also recognized that the concept of entrusting third parties with confidential information is not new or novel. Lawyers already use delivery services, document warehouses and third parties in document discovery efforts.

The Alabama State Bar opined that cloud computing and remote storage of electronic documents are acceptable if certain precautions are in place to provide security and protect confidentiality. Ethics Opinion 2010-02 requires lawyers utilizing cloud services to be informed about how the provider manages the data as well as the security practices used to safeguard the data. Additionally the lawyer should be reasonably sure the provider would abide by the confidentiality agreement, if one exists. Furthermore, lawyers need to stay informed of evolving security practices. If a breach occurs, lawyers will be judged on whether they “acted reasonably in selecting the method of storage and/or the third party provider.”

In Formal Opinion 2010-179, the State Bar of California presented several factors that lawyers should analyze when deciding whether the use of a particular technology is appropriate. Factors to be considered include: (1) the lawyer’s own ability to assess the level of security afforded by the technology, (2) the legal ramifications of unauthorized access, (3) the degree of sensitivity of the information, (4) the impact on the client of an unauthorized access (5) the urgency of the situation, and (6) client instructions and circumstances. Since each particular form of technology can differ in the above elements, lawyers need to evaluate each application of technology and decide whether it can provide the requisite safeguards needed for a particular use.

The California opinion introduces a concept that emerged when the security of email was debated well over a decade ago – that is the client’s input. ABA Formal Opinion 99-413 concluded that when sending highly sensitive information, the lawyer should consult with the client about whether email is appropriate.

Other State Bars have addressed competency regarding lawyers’ use of computers and technology in general. In Formal Opinion 09-04, the Arizona State Bar found that the competence requirement of Rule 1.1 applies to any matter relating to representation. The opinion stated that in order for a lawyer to evaluate the reasonableness of online security, the lawyer must either be competent in online security or consult with someone who is. Furthermore, in Formal Opinion 10-2, The Florida Bar recognized that lawyers need to maintain requisite knowledge and skill, and stay updated on changes in technology in order to identify potential threats to maintaining confidentiality.

ABA Ethics 20/20

While the states have interpreted the ways in which their rules apply to cloud computing and have given direction on what lawyers need to do, the American Bar Association has begun a discussion that may lead to a change of its Model Rules of Professional Conduct and the accompanying comments. In particular, the ABA Commission on Ethics 20/20 has circulated a proposal for discussion that would amend Model Rule 1.6 on confidentiality. The proposal calls for an addition to the rule that would state, "A lawyer shall make reasonable efforts to prevent the unintended disclosure of, or unauthorized access to, information relating to the representation of a client."

The Commission has also proposed an extensive addition to the comment to Model Rule 1.6, giving specific direction on the lawyer's obligation to meet this new requirement. The addition to the proposed comment states:

Factors to be considered in determining the reasonableness of the lawyer's efforts include the sensitivity of the information, the likelihood of disclosures if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty in implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent the client (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 the rule or may give informed consent to forego security measures that would otherwise be required by this rule...

Much like the state ethics opinions, this comment can be broken down into three parts. First, reason prevails. The lawyer is not a guarantor of confidentiality, but merely must make reasonable efforts to assure it.

Second, lawyers must have some knowledge about the systems that they may use. In some cases this may require nothing more than a review of terms of conditions. For example, Google includes in its terms governing Gmail, the statement, "By submitting, posting or displaying the content you give Google a perpetual, irrevocable, worldwide, royalty-free and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any content which you submit, post or display on, or through, the Services." A lawyer may not want to go further than that to conclude that the system will not provide the degree of confidentiality that is needed in virtually any exchange with or on behalf of a client. In other circumstances, the lawyer may need to dive into the level of security or rely on those who can make a valid determination on lawyer's behalf.

Finally, somewhat like the obligation set out when lawyers began to email, the comment suggests the lawyer have a discussion with the client and follow the client's direction to determine the necessary level of security.

Law Practice TODAY

THE MONTHLY WEBZINE OF THE ABA LAW PRACTICE MANAGEMENT SECTION

Once it has completed consideration of all comments, the Commission on Ethics 20/20 will take its proposals to the ABA House of Delegates. The House will then vote on whether to amend the Model Rules.

Conclusion

As long as our duty to maintain confidentiality continues to separate the legal profession from other businesses and services, we will need to take the necessary steps to assure our clients that their information is secure. As our systems of communications become more complex, they become more vulnerable and our duty becomes more difficult. It may be easy to keep a secret, but far more difficult to analyze a system's capability to do so. Nevertheless, we are faced with an increased likelihood that we must take reasonable measures to assure that confidentiality. In some cases those measures may involve a technical assessment of security. Beyond that, we need to incorporate decisions about data management with our clients and abide by their wishes. Confidentiality is, after all, their right and our duty, regardless of how much more difficult it makes our practice management.

Will Hornsby is staff counsel at the American Bar Association. He can be reached at will.hornsby@americanbar.org. The opinions expressed here are his own. Nothing in this article should be construed as the policies of the ABA or any of its constituent entities.

Joseph Duffy is a graduate of John Marshall Law School and is currently pursuing an LL.M. in Information Technology and Privacy Law at John Marshall. He can be reached at JDuffy@law.jmls.edu.