Warning Cloud

Alan S. Wernick, Esq.

There are many benefits available to companies that convert their information technology systems to cloud computing. However, there are many legal issues to consider before converting. One issue that is frequently overlooked is the e-discovery implications.

Introduction

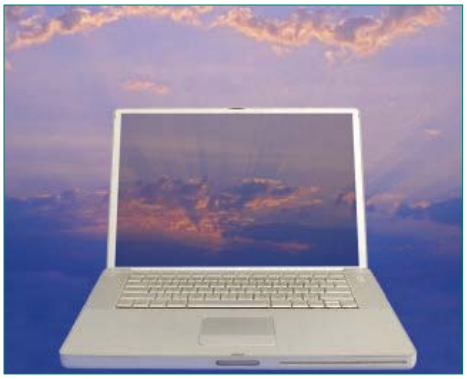
Cloud computing is one of the current waves in information technology. Cloud computing allows the user to transfer many (if not all) of the user's computing functions performed via personal computer applications (and the user's data) to a remote location maintained by the cloud computing service provider. The functions are then accessible by the user through high-speed connections.

Secure Internet connectivity can allow the user access to the cloud virtually anywhere the user has Internet access—whether it's the user's headquarters, an off-site clinic, store, factory, a remote warehouse, a doctor's office, a hotel, a convention center, or home.

Legal Issues Abound

Some companies are hesitant to venture into cloud computing because of the security issues and regulatory compliance issues. Examples of legal issues include the following:

1. E-discovery: What is the impact on evidentiary issues in litigation when the user's data is in the cloud: What data from others is available to your expert?
2. Attorney-client privilege: What impact will storing client confidential materials in the cloud have on the attorney-client privilege? Will the attorney-client privilege be waived by placing such materials in a cloud-computing environment?
3. Privacy, both of the user's data and the user's customer's data: Who establishes, maintains, and audits the access to the user's data and applications in the cloud?
4. Jurisdiction: In case of a data breach, which law applies—that law where the customer is located, that law where the cloud services vendor is located, or that law governing the network or server farm where the data resides? Who has the legal obligation to prepare and send a notice of a data breach?
5. Licensing: If the user uses proprietary third-party applications, do the software license agreements allow for cloud computing usage? This would include not only the scope of use coverage, but other issues as well (e.g., representations and warranties, software maintenance, and upgrade issues).
6. Limitations of liability: If the user signs up for the cloud-computing services through a click-wrap agreement, the terms and conditions are not negotiated. While the click-wrap agreement may be okay in some instances, the cloud-services users may have legal and/or business difficulties with some of the terms and conditions (e.g., the user may find the limitations of the vendor's liability an unacceptable business risk and desire to negotiate different levels and/or triggers of vendor liability).
7. Service level agreements: What are the appropriate service-level agreement terms and conditions? What metric will be used to measure performance in the cloud?
8. Termination: What happens to the user's data if the cloud-services vendor goes out of business or is acquired by a competitor to



the user? If the vendor simply goes out of business, the user could be without access to its business-critical data as well as the applications needed to process that data. Depending on the user's industry, such a scenario could trigger numerous regulatory concerns.

9. Audits: How will the user audit the user's data stored in a cloud-computing environment? How will data quality and data integrity be audited and maintained while in the cloud?

This is not an exhaustive list of all the legal issues, the analysis and determination of which will depend on many factors. These factors include the applicable technology, as well as the business and legal environment for the user and the cloud-services vendor.

Privacy

Privacy in cloud computing is a threshold issue that must be properly addressed in a cloud-computing environment. It cannot be considered in the same light as when all of the computer hardware and software are located at a facility owned and/or operated by the user, and the hardware and software maintained by the user.

For instance, if the user is in an industry, such as the health industry, that relies on substantial data storage:

1. Will the cloud-computing vendor execute a business associate's agreement appropriate to the cloud-computing model?
2. What are the risk allocations in the event of a data breach?
3. Who has the obligation to respond in the event of a data breach (e.g., the user or the cloud computing platform provider)? Which laws apply?
4. How are access controls established and maintained?

Cloudy Discovery

What happens to your data when it's stored in a cloud computing environment?

While there are many nuances to contracting for cloud computing, one aspect frequently overlooked is the e-discovery implications. Often e-discovery is not considered during the contract negotiations because it typically does not arise until some time after the contract has been executed by the parties. For example, when a third party asks the user to produce data stored in the cloud, the request may come as an e-discovery request in the context of a dispute between the user and a third party, or from third parties claiming to have an interest in data that the user controls or has the right to control in the cloud computing environment.

E-mail messages are a familiar example of data that may be stored in a cloud computing environment and may be one of the deliverables in a cloud computing contract. There are many examples of e-mail storage presently being done in a cloud computing environment. In the course of any litigation, access to e-mails will be a necessary part of the e-discovery process. Structuring the cloud computing contract to address the e-discovery issues will save the user time and money when the user has to access those e-mails for compliance or e-discovery purposes.

Summary and Conclusion

The cloud two years from now will be very different in terms of accessibility and risks than it is today. And today, not all cloud systems are alike. For instance, some systems include hardware-oriented firewalls, redundant backups, and sophisticated security systems, while some do not. However, because of the potential for IT cost savings and increased accessibility, many companies will not want to wait before jumping into the cloud.

The bottom line is parties should (1) plan ahead in structuring their cloud computing contracts using knowledgeable legal counsel and (2) consider the many legal issues including, without limitation, the e-discovery implications in the design of the deliverables.

Cloud computing offers many efficiencies and potential cost-savings for the business community. It must be approached cautiously, however, lest the cloud become a fog in which the user loses his way and falls from the cloud into a legal quagmire.

Alan S. Wernick is an Information Technology, Intellectual Property, & Privacy/Cybersecurity Lawyer, Arbitrator/Mediator, & Author/Lecturer with accounting/auditing & tech experience. Additional information about his background and experience is available at LinkedIn: www.linkedin.com/in/alanwernick and at WWW.WERNICK.COM. Alan may be reached via e-mail at ALAN@WERNICK.COM; phone: 847-786-1005.

This discussion was adapted from a pair of articles authored by Alan Wernick that appeared in his Info Tech Law column of the May 2009 and September 2009 issues of Chicago Lawyer. Those articles were used with permission.