MAYER·BROWN

Electronic Discovery & Records Management

Tip of the Month

Cloud Computing and Data Privacy

Scenario

A multinational company is negotiating an agreement with a cloud computing provider to maintain and hold all of the company's electronically stored information and data. The general counsel of the multinational company is concerned about data privacy and data protection both in the United States and worldwide.

What is Cloud Computing?

Cloud computing is the use of computing resources, including both hardware and software, that are made available over the Internet by a subscription-based service provider. Because cloud computing is Internet-based, it offers several advantages over more traditional access to a company's data and software. Cloud-based software and files can be accessed "on demand" from virtually any computer with an Internet connection. For example, when email is stored "in the cloud," the contents of a user's email folders may actually be stored in one or more easily accessed Internet-connected servers located around the world. Moreover, because a company that receives cloud computing services does not rely on its own servers, the amount of data that can be stored is unlimited. Finally, because cloud computing services typically are managed by a third-party provider, they have the potential to reduce a company's IT costs by eliminating the need to acquire and maintain expensive hardware and software. For all of the above reasons, many businesses are seeking to take advantage of this still-evolving technology.

Potential Risks: Data Privacy, Data Storage, and E-Discovery

Data privacy is an issue of concern for companies, their IT professionals and legal departments, whether files stay on-site or are stored electronically with a cloud computing provider. For companies considering cloud computing options, it is particularly important to carefully evaluate the provider's policies and procedures to ensure that they provide sufficient safeguards to protect confidential data. The company's lawyers and IT professionals should develop an understanding of the technology so that they can make informed decisions about whether cloud computing provides the level of protection they require.

One specific risk is that electronically stored information (ESI) may be co-mingled with the ESI of another company or of a separate but related corporate entity. Such situations can make it difficult to determine what entity has "possession, custody, or control" of the data and is under an obligation to preserve or produce the data. Moreover, if a cloud computing provider stores data in multiple servers around the world, ESI may be split up among jurisdictions with different data protection and transfer laws, making it difficult to keep track of how to access and retrieve data, and how to keep data private and secure.

ESI stored with a cloud computing provider can also present challenges to the discovery process in litigation. For example, the U.S. Federal Rules of Civil Procedure allow a party to request discovery of ESI in the responding party's "possession, custody, or control." If a company has contracted with a cloud computing provider to maintain and hold its ESI, the company does not have direct control over, or possession of, the ESI. For purposes of discovery, however, the company still has a duty to preserve and produce that data, as long as it has the practical ability to do so.

Tips for Managing Risks

The use of cloud computing should not fundamentally change the way a company handles ESI. No matter where the ESI resides, a company is responsible for being aware of the information that it creates and for governing that information in accordance with applicable business and legal requirements. It is important that the company be familiar with and closely monitor how its information is stored, retrieved, retained and disposed of by its cloud provider. A company should also develop effective procedures for auditing such activities by its cloud provider. At a minimum, the company should make sure it is capturing sufficient data when information is created (including what the information is, who created it, and for what purpose) to properly govern it.

Before signing a service contract with a cloud computing provider, a company should be sure that the contract contains provisions protecting the company's interests and its need to comply with data privacy requirements. Consider the following items when negotiating a service contract:

- Access: The company should have the right to access all ESI "on demand" and in a specified format that is easy to use.
- Control: The company should have the ability to reasonably direct actions of the provider to preserve and produce ESI.
- Cooperation: The provider should be willing to comply with the company's directions regarding its ESI and to comply with any and all legal holds.
- Speed: The provider should agree to cease any data destruction in a timely manner and to produce data with sufficient speed to meet the company's obligations.
- Metadata: The company should inquire as to the form or format in which data will be stored and returned for production during litigation, including whether metadata will be intact.
- Costs: Beyond the subscription price for the service, the contract should address the costs of potential production, as well as potential indemnification policies and attorneys' fees should the cloud provider's failure to comply with the contract terms result in liability for the company.
- Transparency: The contract should address confidentiality, data integrity and availability issues, including whether data will be commingled with the data of other cloud customers.
- Jurisdiction: The company should discuss with the provider where the data will be maintained and should consider whether production of the data might require compliance with data transfer laws or international privacy laws.
- Ownership: The contract should clearly state that the company owns the data.
- Security: The company should inquire about the security measures that the provider has in place to protect data privacy and attorney-client privilege and whether the company will be informed in the event of a security breach.
- Policies: The company should determine whether the provider's policies and procedures could impede the company's obligations to preserve, collect and produce ESI during

litigation.

- Disaster Recovery: The company should have contingency plans in the event the provider was to suffer a server crash or other data loss or go bankrupt or out of business. The contract should stipulate that its provisions will remain in force if the provider is acquired by another company.

The best way to manage the data privacy and security risks associated with cloud computing is to gain a comprehensive understanding of how the company plans to use cloud computing and to establish procedures and contract terms with the cloud computing provider that meet the company's data security and privacy needs.

For inquiries related to this Tip of the Month, please contact Michael E. Lackey at mlackey@mayerbrown.com, Kim A. Leffert at kleffert@mayerbrown.com or Patrick M. Tierney at ptierney@mayerbrown.com.

Learn more about Mayer Brown's Electronic Discovery & Records Management practice or contact Anthony J. Diana at adiana@mayerbrown.com, Michael E. Lackey at mlackey@mayerbrown.com, or Ed Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.
