# Cloud Security and Privacy: A Legal Compliance and Risk-Management Guide, Part 1

By Robert McHale

Date: May 3, 2010

Return to the article

---

In this two-part series, legal expert Robert McHale, author of Data Security and Identity Theft: New Privacy Regulations That Affect Your Business, provides a comprehensive overview of the legal security and privacy risks associated with cloud computing. Part 1 discusses the principal federal and state laws regulating cloud activities. Part 2 provides a practical due diligence checklist companies should consult before entering into a cloud service agreement.

---

While storage of user data on remote servers is hardly a recent phenomenon, the current explosion of cloud computing warrants a closer look at the associated privacy and security implications.

Cloud computing carries with it its own unique risks regarding the privacy, confidentiality, and security of business information, which companies must fully assess before migrating to the cloud. Armed with an appropriate legal compliance and risk-management strategy—and strong, fully-negotiated contractual protections—companies should be able to safely transfer their data and applications to the cloud.

Part I of this article discusses the principal federal and state laws regulating cloud activities, and the legal security and privacy risks associated with cloud computing.

Part II of this article provides a comprehensive due diligence checklist, which includes a critical examination of key terms found in many standard cloud service agreements, for any company considering utilizing a cloud-based service provider.

## U.S. Laws and Regulations Governing Data Security and Privacy

The United States has numerous federal and state data security and privacy laws with implications for cloud computing. Unfortunately, there is not a single, comprehensive legal framework in which the rights, liabilities, and obligations of cloud providers and cloud users

are regulated or defined. Instead, U.S.-based cloud users and providers must rely upon a veritable hodgepodge of (oftentimes) sector-specific laws to evaluate their legal risks and obligations, and the contractual terms between them.

The most notable data security and privacy laws are examined here.

## HIPAA

The federal Health Insurance Portability and Accountability Act (HIPAA) establishes a comprehensive regulatory framework controlling the use and disclosure of individually identifiable health information by "covered entities," principally health care providers and health plans.

Under HIPAA's *Privacy Rule*, a covered entity may not use or disclose protected health information (PHI) unless as permitted or required by the Rule, or as authorized in writing by the individual affected.

Similarly, HIPAA's *Security Rule* is designed to safeguard the confidentiality, integrity, and availability of electronic protected health information (EPHI). The Security Rule sets forth detailed administrative, physical, and technical standards to ensure that, among other matters, only those who are authorized to have access to EPHI will have access.

With respect to disclosure to cloud service providers, covered entities may not store PHI with a provider absent an agreement (a "business associate contract") wherein the provider agrees to be bound by the same HIPAA privacy and security requirements as the covered entity itself.

The business associate contract must further specify that if the cloud service provider receives a subpoena for a patient record that it is storing on behalf of a covered entity, special reporting obligations are triggered. Under HIPAA, covered entities must notify the patient of, and give the patient an opportunity to object to any subpoena requiring disclosure of a patient's PHI.

**Practice Point**

In certain circumstances, HIPAA's substantive requirements could conflict with the cloud provider's terms of service, and a covered entity may potentially violate HIPAA by using such a provider. For instance, a hospital cannot store patients' medical records with a cloud provider if the terms of service allow the provider to publish any information it stores, as this would violate HIPAA. Proper care must be taken by users to ensure that the substantive requirements of HIPAA are not contradicted by the cloud provider's terms of service.

## The HITECH Act

The Health Information Technology for Economic and Clinical Health Act (HITECH Act), enacted as part of the American Recovery and Reinvestment Act of 2009, establishes new breach notification requirements that apply to HIPAA covered entities and their business associates which access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured protected health information (PHI).

In particular, the HITECH Act requires HIPAA covered entities to notify affected individuals, and requires business associates to notify covered entities following the discovery of a breach of unsecured PHI. The notification requirement is only triggered if the breach poses a significant risk of financial, reputational, or other harm to the affected individual.

Prior to disclosing PHI to cloud providers, organizations should ensure (as part of their contract) that the provider will observe the breach notification requirements under the HITECH Act.

**Practice Point**

The HITECH Act authorizes each state's attorney general to file lawsuits, on behalf of their residents, to enforce HIPAA's privacy and security protections, and imposes increased civil monetary penalties for security breaches. In light of this more strident regulatory environment, covered entities need to exercise extra vigilance in safeguarding PHI, and in providing prompt notice if a breach occurs.

## Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA) has two key provisions carrying significant privacy implications for "financial institutions" storing data in the cloud: the *Financial Privacy Rule* and the *Safeguards Rule*.

**Practice Point**

"Financial institutions" include not only banks, securities firms, and insurance companies, but also companies providing many other types of financial products and services to consumers, such as lending, brokering or servicing consumer loans, preparing individual tax returns, providing financial advice or credit counseling, and collecting consumer debts.

*The Financial Privacy Rule* governs the collection and disclosure of customer's personal information by financial institutions, and by any company, regardless of whether they are a financial institution, who receives such information. Under the Financial Privacy Rule, prior to disclosing consumer personal information to a service provider (including cloud providers), a financial institution must enter into a contract with the service provider prohibiting the service

provider from disclosing or using the information in any manner other than to carry out the purposes for which the information was disclosed.

The Financial Privacy Rule also requires financial institutions to provide their customers with a privacy notice at the outset of their relationship, and annually thereafter, explaining how their personal financial information is being collected, shared, used, and protected. The notice must also state that customers have the right to opt out of having their personal financial information being shared with nonaffiliated third parties.

**Practice Point**

Whether a cloud service provider will be deemed an "unaffiliated party" for purposes of GLBA's Financial Privacy Rule has yet to be determined. Financial institutions using a cloud as a platform for their services may find themselves in an untenable, *Scylla and Charybdis*-like position should the cloud provider be deemed a nonaffiliated third-party and should the customer elect to "opt-out" of having their information so shared.

*The Safeguards Rule* requires all financial institutions to develop, implement, and maintain a "comprehensive information security program" to protect nonpublic customer information. The Safeguards Rule require financial institutions to periodically monitor and test their security program, and to update the safeguards as needed with the changes in how information is collected, stored, and used. Further, prior to allowing a service provider access to customer personal information, the financial institution must:

- Take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue.
- Require the service providers by contract to implement and maintain such safeguards.

Given the complex administrative, technical, and physical information safeguards requirements imposed by the GLBA, managing the risks associated with nonpublic information stored in the cloud may prove particularly challenging.

## USA PATRIOT Act

The USA PATRIOT Act provides authority for law enforcement agencies to compel disclosure of virtually any document, including electronic documents held by cloud providers.

Section 215 of the Act permits the issuance of *ex parte* Magistrate Judge court orders:

> "The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such

> investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."

Further, those who receive a Section 215 court order are severely restricted in their ability to reveal to others that they received such an order, or to alert the subject of the order that the order was received. Problematically, those who use cloud providers to store or process their data may not even know that the government obtained their records.

Likewise, pursuant to Section 505 of the Act, the FBI may demand, through the use of National Security Letters (NSLs), personal customer records (including e-mails, financial records, and consumer reports) from financial institutions and wire or electronic communication service providers without any prior court approval.

Because any electronic data stored in the United States is potentially subject to *ex parte* governmental disclosure, a few foreign governments (most notably the Canadian provinces of British Columbia and Nova Scotia) have enacted various restrictions and/or prohibitions regarding the cross-border transfer of information with U.S.-based cloud providers.

**Practice Point**

Section 215 of the Patriot Act is set to expire on February 28, 2011. Orders entered prior to that date are still valid, however, and the point regarding *ex parte* access to information remains a concern. Governments, organizations and businesses may continue to elect not to store or process data with cloud providers located in the United States for fear that such information may be potentially exposed.

## Electronic Communications Privacy Act

The Electronic Communications Privacy Act (ECPA) sets out provisions for the access, use, disclosure, interception, and privacy protections of electronic communications.

Generally speaking, the ECPA proscribes the unauthorized access of electronic communications service facilities, and any electronic communications in storage. The ECPA also prohibits "electronic communications service providers" from divulging the contents of such communication while it is in electronic storage.

Additionally, the law prevents government entities from requiring disclosure of electronic communications, such as email messages, from a provider without proper procedure (for example, via a trial subpoena or warrant).

Despite the strict mandates against disclosure, use of cloud service providers carries some risk, as there have been many instances where service providers have been compelled to disclose information upon receipt of a court order.

It has yet to be established whether the protections available for information in the cloud against a governmental demand for disclosure is or is not greater than those available for records held by third parties. In light of this uncertainty, measuring the risk involved with cloud computing against governmental demands for information is difficult.

**Practice Point**

The level of protection afforded any given cloud activity may be a function of the cloud activity itself. For example, within the ECPA framework, certain e-mails held in “electronic storage” by an “electronic communications service” could only be accessed by law enforcement with a warrant (which requires probable cause), whereas a subpoena alone (which does not require prior judicial approval) would be sufficient to access the same e-mail if “stored” by a “remote computing service.”

## E-Discovery and the Federal Rules of Civil Procedure

Under Rule 26 of the Federal Rules of Civil Procedure, all parties to a federal lawsuit are required to disclose (without awaiting a discovery request) a copy of all electronically stored information (ESI) that the disclosing party has in its possession, custody or control and which it may use to support its claims or defenses.

(Some states have adopted similar rules for e-discovery for lawsuits at the state level.)

A party is required to produce the ESI in the form(s) in which it is ordinarily maintained or in reasonably usable form(s), or in the form specified in the request for production.

Businesses must take measures to preserve ESI not only at the inception of a lawsuit, but whenever litigation is reasonably anticipated. In this regard, parties are required to initiate a *litigation hold* and cease from further destruction of a company’s documents which may be relevant to a lawsuit.

**Practice Point**

Considering that multiple copies of data may be created, stored, recompiled, dispersed, reassembled, and reused, determining what constitutes a "record" or a "document" for discovery purposes may be difficult to achieve in the cloud.

The legal requirements imposed by the Federal Rules of Civil Procedure on litigants who store information in the cloud can therefore be quite problematic, as otherwise discoverable and relevant data may not be easily accessible by the parties’ cloud service providers, may not be properly preserved, or may be inextricably intertwined with others’ data so as not to be produced without compromising the privacy of others. To avoid this issue, companies should acquaint themselves with their cloud service provider’s retention policies, and be confident

that if a litigation hold needs to be initiated, their data will be properly segregated and retained.

**Practice Point**

Serious penalties exist for certain failures to produce ESI. Is the loss of ESI due to a routine, *good-faith* operation of an electronic system? If not, significant sanctions may be imposed for failure to produce ESI—including dismissal of your case, or a default judgment in favor of your opponent. A company's retention policies, together with its routine destruction cycles, must be well documented to avoid the possible inference that any loss of ESI was the result of *bad faith.* In this regard, whenever litigation is "reasonably anticipated", the destruction of a company's ESI should be immediately suspended to avoid the negative inference.

## Massachusetts Data Security Regulations

In 2007, Massachusetts mandated the adoption of detailed information security regulations in order to reduce the number of data security breaches.

The resulting regulations, 201 CMR § 17.00 *et seq*. (effective March 1, 2010), impose detailed administrative and technical obligations on any person that owns, licenses, stores or maintains "personal information" of Massachusetts residents (for example, name and Social Security number, financial account number or credit card number). The regulations also impose significant technical requirements for any computers, systems, or networks involved in the maintenance or transmission of personal information.

Companies subject to the Massachusetts regulations must take reasonable steps to ensure that third-party service providers (including cloud providers) with access to personal information have the capacity to protect such information consistent with the Massachusetts regulations and applicable federal regulations.

Companies must also require that their third-party service providers contractually agree that they have appropriate security measures for personal information.

It is important to note that the Massachusetts regulations apply to any business, whether or not operating in Massachusetts, handling personal information of Massachusetts residents. In the cloud context, companies need to ensure that their cloud providers maintain appropriate security measures to protect stored data involving personal information of Massachusetts residents.

**Practice Point**

Many states have enacted data breach notification laws, requiring companies to publicly report the unauthorized acquisition or use of compromised data. In a cloud environment, it may be logistically impossible for a data owner to confirm security conditions at every server

location that may be involved in the storing of its data. Further, without adequate control over the reporting obligations of a cloud provider, cloud users may simply be unable to fulfill their notification requirements in the event of a cloud-based data breach.

## The European Union Data Protection Directive

The location of information stored in the cloud can have a profound impact upon the level of privacy and confidentiality protections afforded the information in question, and upon the privacy obligations of the cloud provider.

For instance, the European Union's Data Protection Directive, which regulates the processing of personal data within the EU as a means to safeguard individual citizens' privacy, is of particular significance.

Under the EU Data Protection Directive, personal data may be transferred to third countries (non-EU member states) only if that country provides an "adequate" level of protection. Most notably, the United States is *not* on the list of countries that meet the EU's "adequacy" standard for privacy protection. Accordingly, an organization that does its processing in the cloud may be violating EU law if the data goes to a server outside of the EU to prohibited countries, such as the United States.

In order to provide a means for U.S. companies to comply with the Directive (and thereby ensure continued trans-Atlantic transactions), the U.S. Department of Commerce, in consultation with the European Commission, developed a "Safe Harbor Program" designed to protect accidental information disclosure or loss.

U.S. companies can opt into the program and self-certify as having "adequate" privacy protections, provided they adhere to the following seven Safe Harbor principles:

- **Notice**: Organizations must notify individuals about the purposes for which they collect and use their information. Individuals must also be notified about the types of third parties to which the organization discloses the information, and the choices and means the organization offers for limiting such disclosure.
- **Choice**: Organizations must give individuals the ability to opt out of the collection and forward transfer of their data to third parties.
- **Onward Transfer**: Organizations may only transfer information to a third party if the third party subscribes to the Safe Harbor principles, or is subject to the Directive. Alternatively, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Safe Harbor principles.
- **Access**: Individuals must be able to access information held about them, and correct or delete it if it is inaccurate.

- **Security**: Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration, and destruction.
- **Data Integrity**: Data must be relevant and reliable for the purpose it is to be used.
- **Enforcement**: There must be effective means of enforcing these rules, verifications that an organization's commitments to adhere to the Safe Harbor principles have been implemented, and obligations to remedy problems arising out of failure to comply with the principles.

**Practice Point**

A company's failure to abide by its commitments to implement the Safe Harbor principles may be actionable under federal and state law prohibiting unfair and deceptive acts. This is the case even when an organization adhering to the Safe Harbor principles relies entirely on self-regulation to provide the enforcement required by the Safe Harbor enforcement principle. The Federal Trade Commission has the authority to rectify such misrepresentations by seeking administrative orders and civil penalties of up to $12,000 per day for violations.

Continue reading this article in Part II.

## Final Note

The information contained herein is not intended to constitute legal advice or a legal opinion as to any particular matter. The contents are intended for general information purposes only, and you are urged to consult with an attorney concerning your own situation and any specific questions you may have.

***Robert McHale, Esq.*** *is the founding Partner of R | McHale LLC, a full-service law firm whose corporate practice represents clients on a wide variety of IT and intellectual property law matters, including privacy and data security, copyright, trademark, licensing, and other proprietary protections.*

*He may be contacted at: robert.mchale@rmchale.com*

---

# Cloud Security and Privacy: A Legal Compliance and Risk-Management Guide, Part 2

By Robert McHale

Date: May 10, 2010

Return to the article

---

In this two-part series, legal expert Robert McHale, author of Data Security and Identity Theft: New Privacy Regulations That Affect Your Business, provides a comprehensive overview of the legal security and privacy risks associated with cloud computing. Part 1 discusses the principal federal and state laws regulating cloud activities. Part 2 provides a practical due diligence checklist companies should consult before entering into a cloud service agreement.

---

## Due Diligence and Cloud Service Agreements

An organization's contractual agreement with a cloud service provider is perhaps the most critical component in evaluating cloud computing risks, and therefore should be carefully examined before being entering into a cloud relationship.

Cloud Service Agreements (CSAs) should clearly describe the services provided, guarantees, warranties, limitations, liabilities, and the responsibilities and rights of each party.

Proper due diligence requires inquiry into the following categories of concern: data security, performance, limitations of service, data migration, government and third-party litigation access, handling of trade secrets/confidential information, and exit plan, all of which are discussed in detail below.

### Data Security

To properly manage the operation risk associated with cloud services, the cloud provider's level of data security should be carefully examined. At a minimum, the following should be ascertained:

- Is the cloud provider contractually obligated to protect the customer's data at the same level as the customer's own internal policies?
- Who has access to customer data, and what are their backgrounds?

- Where is the provider's data center physically located, and what safeguards exist to prevent data centers from unauthorized access (for example, 24/7 security personnel)?
- Does the provider promise to maintain user data in a specific jurisdiction and/or to avoid certain jurisdictions?
- What are the provider's migration policies regarding moving data back internally or to alternate providers? (Companies need to make sure that no data is lost or falls into the wrong hands.)
- Does the provider conduct regular backup and recovery tests?
- Do the provider's security policies comply with all applicable regulatory rules?
- Is the provider willing to undergo on-demand or periodic audits and security certifications?
- Is the provider required to investigate illegal or inappropriate activity?
- Is the provider required to disclose any new vulnerabilities that may affect the confidentiality of customer data, or the integrity and availability of their services?
- In the event of lost or compromised data, can the data be backed up, and can it be easily reconstituted from the backups?
- What are the provider's policies on data handling/management and access control? Do adequate controls exist to prevent impermissible copying or removal of customer data by the provider, or by unauthorized employees of the company?
- What happens to data when it is deleted?
- What happens to cloud hardware (for example, trailers of servers) when the hardware is replaced?

**PRACTICE POINT**

The security and privacy risks associated with cloud computing are exacerbated when the cloud service provider reserves the right to unilaterally change the terms of its privacy policy and terms of use. By rejecting such unilateral change provisions, users can avoid having their carefully negotiated risk allocations taken away.

## Performance

For many companies, the continued availability of cloud services is of critical importance. The inability to access data stored in the clouds can cause significant business interruption, lost revenue and lost goodwill. Before entering into a CSA, be sure to obtain satisfactory answers to the following questions:

- Does the provider have multiple power feeds from separate sources?
- Does the provider have multiple communication links from diverse suppliers (in order to safeguard against service disruption due to connectivity problems)?
- Has the provider paid out any service-level credits in the past six months, and if so, what were they paid out for?

- Have any of the provider's customers experienced an interruption in service, and if so, for how long?
- Is the provider able to continuously provide services (and access to customer data), even around scheduled service downtimes?
- Can the provider seamlessly transfer customer data to an alternate supplier, if the need arises?
- Are there special circumstances known to the provider which make an interruption of services a reasonable possibility? (For instance, is the provider undergoing financial difficulty? Is it relying upon a financially troubled sub-contractor? Is it involved in litigation?)
- In the event of data loss, how quickly will the provider perform data restores?
- What liability (if any) does the provider have to the user in the event of interruption of service or loss of data due to a *force majeure* (such as war, government sanction, embargo, or power outage)?
- What is the provider's contingency plan in the event of a natural disaster? For example, does the provider have the means to quickly transfer customer data and redeploy customer applications to a secondary location?
- What contractual obligations (if any) will the provider assume regarding uptime, and are any uptime warranties included?

## Limitations of Service

CSAs frequently contain several exclusionary clauses that should give companies contemplating migrating to the cloud significant reason to pause. Such clauses should be carefully scrutinized and, where appropriate, qualified or deleted. The most onerous clauses are identified below.

- The unilateral right to limit, suspend, or terminate the service (with or without notice) (and for any reason)
- Disclaimer of liability relating to service quality and availability
- Disclaimer of all warranties, including the implied warranties of merchantability and of fitness for a particular purpose
- Disclaimer of liability for third-party action
- Remedy limitations, including total damages capped (such as a return of fees paid), and/or exclusion of consequential damages (such as loss of profits/revenue)

**PRACTICE POINT**

The broad exclusionary clauses found in many CSAs may prove to be a cloud provider's contractual undoing. Federal and state consumer protection laws may very well frown upon a provider's claims of effective service, reliability, and security on the one hand, if the provider simultaneously disclaims quality and performance on the other.

## Data Segregation

Currently, most cloud service providers offer their services on a shared server basis. Special care should be taken to ensure that your company's data is not inadvertently mingled with that of a competitor's. The following questions should be asked to ascertain the provider's data segregation procedures:

- What procedures does the provider have in place to ensure that a competitor does not have access to customer data, even if both customer and competitor are hosted on the same server?
- How frequently does the provider monitor its server to confirm that data is properly segregated?

## Governmental and Third-Party Litigation Access

The CSA should clearly state how the cloud provider will respond to legal requests for information, and what notice and opportunity for objection the cloud user is granted. For instance:

- Is the provider required to notify the user if the provider receives a subpoena, search warrant, or other lawful request for user information?
- Will the cloud provider seek a protective order to prevent and/or limit disclosure of company data?
- In the event of litigation, how are litigation holds enforced? What are the procedures to make sure user data is segregated and retained?
- How are e-discovery requests handled? How is metadata protected? And how is information searched for and retrieved?
- Which party bears the costs associated with processing data for discovery purposes?

## Trade Secrets and Confidential Information

The CSA should include a provision to maintain the confidentiality of a company's trade secrets and proprietary information, although even then storage of a company's trade secrets with a cloud provider carries significant risk.

Under the Uniform Trade Secrets Act, for a company's proprietary information to be accorded trade secret status, the trade secret must be, at a minimum, the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Whether a transfer of trade secrets to a cloud provider extinguishes the trade secret has yet to be ruled upon. A company's trade secrets may lose their status as such even in

circumstances where the cloud provider commits to keeping confidential any information it receives.

Certainly, where the cloud provider's terms of service allows the provider to see, use, or disclose information, this would probably vitiate the user's claim that the information is a trade secret.

**PRACTICE POINT**

Storing trade secrets in the cloud carries an additional risk from a jurisdictional perspective. If the law of trade secrets in the jurisdiction where a user's data is stored is less protective of information than the law in the jurisdiction where the user is physically located, a user may be required to seek enforcement of his trade secret rights in an "unfavorable" jurisdiction. Furthermore, data held in another country may be more vulnerable to government access than the same data held in the user's home country. Compounding these risks is that fact that the location of the "cloud" is not always readily ascertainable, and is oftentimes multi-sited and subject to change.

Likewise, the CSA should be reviewed to determine whether privileged communications remain intact.

Generally speaking, privileged communications, such as those of a client to his or her attorney, are destroyed if shared with third parties.

If the CSA allows the provider to read, use, or disclose the information, then privilege will most likely be lost. If, on the other hand, the CSA allows the provider only to store the information, without the right to look at the information, then the privilege probably survives the transfer of the data to the provider.

## Exit Plan

An exit plan defining each party's obligations in the event of a termination of services should also be clearly set forth in the CSA. For instance,

- How long after termination of service will customer data be returned to the customer, and in what form?
- Is the provider required to assist the customer in transferring data to a new provider or back to a self-managed platform?
- Is the provider required to maintain a backup copy of customer data post-termination in perpetuity, or is all customer data to be destroyed within a certain time frame?
- How is customer data disposed of at the end of the relationship with the provider?
- What happens to customer data in the event the provider goes out of business?
- For encrypted data, how is the data to be decrypted when it is returned?

- Can the user's data and applications be readily transferred to and from the cloud so as to avoid being locked in to any particular cloud vendor?

Naturally, as cloud services become consolidated into only a handful of big players, the ability to negotiate the terms of a CSA will become increasingly difficult. Nonetheless, given the current stage of robust cloud competition and consumer skepticism regarding cloud safety, the ability to negotiate terms is at a relative high point. Companies should leverage this fact to insist upon terms that maximize protection of their data and minimize their legal risks.

**PRACTICE POINT**

Achieving contractual protection in the cloud can be complicated by the fact that users do not always have a direct relationship (and therefore enforceable contractual privity) with all relevant players. For example, an organization may retain an SaaS cloud provider for remote desktop backup services, but the data itself may be stored and processed by others, at the IaaS or PaaS level. As part of the due diligence of their direct provider, companies should require confirmation that the direct provider also conducted an adequate due diligence of all related service providers. In this regard, companies should insist on reviewing the contract their direct provider has with any secondary provider to ensure regulatory compliance is maintained, and that no additional legal risks or obligations may be created.

## Conclusion

Significant benefits are associated with adopting cloud services, including lower costs, less need for on-site support, and scalability.

Migrating to the cloud also carries with it its own unique data security and privacy risks, and legal and regulatory compliance obligations.

Due diligence of the service provider, together with a carefully drafted service agreement specifying each parties' rights, obligations, and liabilities, are perhaps the most critical risk mitigation measures a company can adopt before deploying into the cloud.

## Final Note

The information contained herein is not intended to constitute legal advice or a legal opinion as to any particular matter. The contents are intended for general information purposes only, and you are urged to consult with an attorney concerning your own situation and any specific questions you may have.

***Robert McHale, Esq.*** *is the founding Partner of R | McHale LLC, a full-service law firm whose corporate practice represents clients on a wide variety of IT and intellectual property law*

*matters, including privacy and data security, copyright, trademark, licensing, and other proprietary protections.*

*He may be contacted at: robert.mchale@rmchale.com*

---