continued from page 5
should be carved out from its effect. A company should avoid becoming liable to third parties for damages arising from the contractor's acts without solid indemnification rights to recoup payment for those losses.

Indemnification Provisions

Indemnification provisions demand a close look. Many times, the service provider will try to severely limit its indemnification obligation. For example, a party may seek to limit indemnification obligations to claims made only as a result of gross negligence. Simultaneously, the contract may tie the indemnification provisions to the limitation of liability provisions. As such, the company can be left with substantial third party claims for damages caused by the service provider with little or no indemnification rights. Generally, it's a good practice to clarify that any indemnification will be triggered for, at the very least, the provider's negligence, intentional misconduct, or breach of the agreement. If possible, the indemnification should be expanded to include all "loss" as opposed to just third party "claims," thus removing a pre-condition that a claim must have been made before indemnification is available. The provision should always specify that the indemnification obligation survive the termination of the agreement to avoid expiration at the end of the contract term.

It is generally best to include an affirmative duty to defend in the indemnification provision. Without a specific duty to defend, an indemnification provision is less valuable. Recently, consultants have been aggressive in pushing back on their duty to defend. There is an argument to be made (most often by insurance carriers) that if a consultant defends a third party in situations in which there is no negligence on the part of the consultant, the insurer may deny coverage for the cost of that defense. The argument is that a contractual duty to defend a third party does not trigger coverage unless a covered act by the consultant is ultimately adjudicated to have occurred. It is preferable to allocate this risk to the consultant and negotiate that the duty to defend remain. A compromise position would be to provide for defense cost reimbursement if the consultant is found negligent. The defense cost can therefore be characterized as an additional damage amount caused by the consultant's covered negligence. This is not optimal as it does leave a gap in the defense cost indemnification as the consultant's contractual duty to defend is no longer broader than the duty to indemnify. It is, however, a better result than elimination of the duty to defend that many service providers are now trying to negotiate into their contracts.

Conclusion

The effect of these provisions is not inconsequential, and the provisions are often overlooked or misunderstood. While there are many factors to consider in deciding whether to negotiate some or all of these terms, it's beneficial to know what rights are in play.

In-house Counsel in the Cloud – Can You Trust Online Storage?

By Christopher Hopkins, Akerman Senterfitt

Most corporations suffer from data storage burdens and struggle with concerns about employees' remote access to files. Moreover, secure and reliable email transmission is a frequent problem when corporate email systems commonly block large email attachments above 5-10 mg. Often, lawyers and other personnel find that they cannot simply attach large PDFs to emails due to size restrictions. Increasingly, the solution rests in third party "cloud" storage providers. It could be a private cloud, where the company's entire system is hosted online, or a public cloud, such as Dropbox, which helps individually send or remotely access a subset of their files. The risk, however, is that cloud storage is an emerging technology with unclear legal and practical boundaries.

In March 2012, the Fraunhofer Institute reported its study of the security methods of several cloud providers (bit.ly/M0Rvdu). Fraunhofer is likely an unfamiliar name but it is a massive, well-respected German research society which created, among other things, the MP3 music file format. Ironically, the study results are limited since (a) they examined only seven cloud providers, (b) there was no clear winner, and (c) any cloud updates after the study changes the results. Instead, the study raises awareness of the points where danger can arise. Here are some initial considerations before your corporation leaps into the cloud.

Is the "Cloud" Inherently Dangerous?

Lawyers often think of security in terms of preserving the corporation's confidentiality. Some counsel fear that email is unsecure but common business practices have galvanized the acceptance of email. The legal concept of "confidentiality" rests on the notion that third parties have been excluded. Leaving files with a third party requires some steps before confidentiality is achieved. Businesses rely on third party shipping and storage companies in the physical world; simply because we do so in the virtual world should not be cause for blind panic.

Reasonable concern, however, arises from the fact that digital transmission and storage of confidential information involves numerous third parties, known and unknown, as files travel over wifi or cell networks, through ISPs and email services, and across the various intermediary nodes of the internet. Before engaging a

continued on page 7

continued from page 6

cloud service for the corporation, counsel need to ask what security is used during transmission and storage; if you do not understand the terminology, begin with a Google search to see how the IT community views the proposed security methods and then consult your company's IT professionals with a list of questions. Despite a cavalcade of news stories about hackers, data loss, and downtime, the general consensus is that responsible cloud computing is reasonably secure.

Where Is Your Cloud Located?

We call it a "cloud" but your data is stored terrestrially, somewhere. Consideration should be given to whether your data is stored domestically or internationally. If your provider is outside of the U.S., be aware of export laws, application of non-U.S. laws, seizure by foreign governments, and enforcement of your contract rights (to say nothing of slow latency in your internet connection). Inside the U.S., providers are subject to the Patriot Act but you also have Fourth Amendment rights. There are jurisdictional considerations – will the location of your cloud-stored data create a "presence" where your company does not want one? Also, what happens if the cloud provider's servers are seized due to the actions of another client? Some redundancies, beyond a single cloud, may be in order. Finally, even with redundancies, make sure that a single natural disaster (e.g., a hurricane in Florida) does not risk both your cloud and your local data.

Trust… But Verify

When storing data with a third party, you should consider encrypting your files. First, make sure that the connection between your company and the cloud is secure through HTTPS or some other transport layer security. Second, ensure that the cloud stores your files in an encrypted format. Encryption can be done before data is transmitted to the cloud ("client-side" encryption) and/or upon arrival in the cloud ("server-side" encryption). Either way, there is the risk that the client (your company employees) might lose their password or that the company might fail to limit access. With server-side encryption, there is the concern that a third party (malicious or not) has access to your data and that you may lose control of once-encrypted data if your provider receives a formal demand for access to your data. To this end, client-side encryption may be preferred.

File Sharing Risks

Often you need to send a large file via email but your company's system, or the recipient's, declines a file over a certain size. The workaround is to use a cloud to store the file and then you simply email the file's URL address. Using DropBox, for example, you can open specific files so that others have access.

If your cloud has this service, make sure that the file's URL address does not contain information about your company or the filing structure, which might betray hints about other data (Fraunhofer recommends that the cloud generate a "unique identifier" in the URL). There should be a time limit to how long it is accessible and the cloud provider should ensure that the file is not so public that it can be indexed by Google.

For corporate counsel, DropBox may be a quick, individual solution but it is not necessarily a desired practice to have individual employees using personal clouds to transmit corporate data. If personnel are experiencing problems with email attachment limitations, this may be a signal that it is time to consider a formal policy and/or a cloud solution.

In-house Counsel Guide to Cloud Contracts (SLA)

Cloud computing contracts, more formally known as Service Level Agreements (SLA), should be considered and negotiated with the involvement of both counsel and corporate IT professionals. SLAs involve technical issues in an emerging technology. Moving files to the cloud is not necessarily limited to a corporation seeking extra storage space. Some forward-thinking needs to be given to collaborative development; e-discovery and e-rentention needs; and regulatory compliance. Even for the technology-inclined lawyer, "software as a service" (SaaS) may be a new concept.

For the lawyer, primary issues to consider are confidentiality, reliability, searchability, ownership rights, and scalability. An IT professional will assess the provider's security methods, transmission and access claims, and other content management issues. Both counsel and IT will want to assure themselves that the cloud provider has a reliable track record and has satisfied clients in regulated industries like healthcare or finance. Moreover, both lawyer and IT professional need to work together to ensure that data is indexed, searchable, and can "scale" as the company (and its data) expands.

Cloud computing does have it limits. In November 2009, Google outbid Microsoft for a cloud computing agreement with the City of Los Angeles to provide email and Google Apps for city employees. Since that time, there has been continued concern over regulatory and security compliance, resulting in the Los Angeles Police Department declining to move its personnel to the cloud due to security concerns. As an initial step, counsel should review the Google-Los Angeles SLA (*http://bit.ly/QbdAi2*) as well as other government SLAs (*http://bit.ly/Qbe4Vb*).

Common Pitfalls in Selecting Cloud Providers

When seeking cloud providers, counsel needs to become educated about the technology and consult the company's IT professional about its specific needs. When seeking bids, counsel needs to obtain marketing material, technical specifications, and proposed SLAs. Security, latency, and uptime are critical components but however cloud computing contracts require special focus on remedies — if relying on a modest to moderate cloud provider, will it have insurance or the resources to remedy damages? Alternatively, consider reputation penalties where the provider must post its service level performance. Finally, once in place, both corporate counsel and IT need to monitor the cloud's performance.

Recommendations

Digital file retention requires reasonable precautions and redundancies. But cloud computing also involves searchability, collaborative access, and, for counsel, the ability to satisfy e-discovery and regulatory requirements. For cloud storage: (a) keep a reasonably up-to-date secondary backup in a separate location, (b) consider

continued on page 8

continued from page 7

client-side encryption before your data is sent, and (c) ensure responsible password and access protocols are followed at your corporation.

***Christopher Hopkins** is shareholder at AkermanSenterfitt in West Palm Beach, Florida. He can be reached at christopher.hopkins@akerman.com.*

The Patient Protection and Affordable Care Act Is Constitutional. So Now What, and Will It Be Repealed?

By Dana Thrasher, Bob Ellerbrock and Evan Gibbs, Constangy, Brooks & Smith, LLP[1]

On June 28, 2012, the Supreme Court of the United States issued its landmark 5-4 decision in *National Federation of Independent Business v. Sebelius*, widely regarded as one of the most important and far-reaching decisions in decades. The Court held that neither the Commerce Clause nor the Necessary and Proper Clause of the Constitution allowed for the imposition of the individual mandate included in the Patient Protection and Affordable Care Act (the "Act"). Ironically, while both Congress and President Obama previously maintained that the monetary cost of noncompliance with the mandate was not a tax, the Court found that the individual mandate was constitutional under the Taxing Clause. The Court's ruling that it was a tax seems in contradiction to the Court's precedent regarding the Anti-Injunction Act of 1867, which precludes any court from considering the imposition of a federal tax prior to its enforcement. The Court, however, found the Anti-Injunction Act was inapplicable because the individual mandate was intended to be a penalty and not a tax.

Since the Court found the Act constitutional, it is not only important for Corporate Counsel to recognize and understand some of the major changes slated to go into effect, but also the chances of the Act being repealed.

CONSTANGY
BROOKS & SMITH, LLP
The Employers' Law Firm, Since 1946

What Should Employers Focus On?

Based on the Court's ruling, Corporate Counsel should continue to work with their companies towards compliance with the Act. Although this article will not address all of the changes under the Act (particularly those which should have already been implemented), the scope here will instead focus on describing a few of the major mandates that will soon become effective:

- **Summary of Benefits and Coverage** – For any open enrollment periods beginning on or after September 23, 2012, group health plans must provide employees with a new notification called a Summary of Benefits and Coverage (SBC). The SBC is intended to focus on available coverages, cost-sharing provisions, benefit limitations, and similar issues. Group health plans must provide an SBC on an annual basis, typically during each open enrollment period. Failure to provide an SBC may result in a penalty of up to $1,000 per enrollee/participant.
- **W-2 Reporting Requirements** – Employers must report the value of employees' health coverage on annual W-2 forms. This requirement is effective for the 2012 tax year, so W-2 forms issued in January 2013 should include this information. Employers which issue fewer than 250 W-2 forms are currently exempt.
- **Changes to Health Care Spending Accounts** – Effective January 1, 2013, the definition of a "qualified medical expense" will be narrowed. This will affect reimbursements and withdrawals under all types of health care accounts, such as flexible spending accounts, health reimbursement arrangements, health savings accounts, and Archer medical savings accounts. Over-the-counter medications will no longer be a "qualified medical expense." Additionally, the amount employees may contribute to health care flexible spending accounts will be capped at $2,500.
- **Penalty for No Coverage Offered** – Beginning in 2014, "applicable large employers" (with more than 50 full-time equivalent employees) that do not offer any group health coverage and have at least one full-time employee who receives coverage through an Exchange will be assessed a penalty. The penalty is calculated as $166.67 per month (1/12 of $2,000 annual penalty) multiplied by the number of full-time employees in that month, excluding the first 30 employees. For purposes of determining whether an employer is an applicable large employer, an employer must include not only its full-time employees but also a full-time equivalent for employees who work part-time. In addition, applicable large employers that offer group health coverage but still have at least one full-time employee receiving a premium tax credit (toward

continued on page 9

---

[1]*Dana Thrasher is a partner and Bob Ellerbrock is an associate in the Birmingham, Alabama office, specializing in Employee Benefits Law. They can be reached at (205) 252-9321.*

Evan Gibbs is an associate in the Jacksonville, Florida Office. He can be reached at (904) 356-8900.

To learn more, please visit www.constangy.com.