Transcending the Cloud

A Legal Guide to the Risks and Rewards of Cloud Computing

ReedSmith

reedsmith.com

— CLOUD COMPUTING TASK FORCE LEADER —

Joseph I. Rosenbaum
Partner and Chair, Advertising Technology & Media Law Group
jrosenbaum@reedsmith.com
+1 212 702 1303

— EDITOR —

Joseph I. Rosenbaum – jrosenbaum@reedsmith.com

— TABLE OF CONTENTS —

Reed Smith Cloud Computing Initiative

"I've looked at clouds from both sides now
From up and down and still somehow
It's cloud's illusions I recall
I really don't know clouds at all"[1]

Unless you have been living in a fog, you could not have escaped hearing about Cloud Computing. At the risk of spoiling the surprise, Reed Smith created this Cloud Computing initiative, based on our observations and growing belief that Cloud Computing is and will continue to fundamentally alter the business, economics and operations of companies around the world. Cloud Computing is not a technological phenomenon any more than Social Media is a technical innovation. Cloud Computing, like Social Media, is driven and enabled by technology, but represents a fundamental significant shift in the manner in which technology will be used by everyone in the years and decades ahead. The result will be shifting and unique legal and regulatory challenges. We will see fundamentally different business, economic and operational relationships between providers and business enterprise, between business enterprise and customers, between suppliers and business enterprise and customers, and even internally within each business enterprise itself. In the months that follow, we aim to dig well below the surface of many of the legal, regulatory and contractual implications presented by Cloud Computing.

So what do we mean by "Cloud Computing"? One of the simplest definitions I've seen, comes from a 2010 Yankee Group report[2], that defines "cloud computing" as "dynamically scalable virtualized information services delivered on demand over the Internet." Unless you are extraordinarily conversant with the technology, that definition might leave you a bit numb. So let me give you a few analogies that might be helpful.

You buy a toaster and plug it into the wall socket. The utility company hasn't a clue you bought it, nor do they know if it's a small one or a commercial grade toaster. You didn't use it today, but tomorrow you will. You also have an air conditioner that's on a thermostat—it cycles on and off depending on the temperature. You might live in a single-family home or an apartment house with more than 100 units. The electricity demands may vary greatly by unit or even by individual, and within a few miles or a few thousand miles, the ebb and flow of demand for electricity is locally unpredictable and dynamically variable. But through years of capacity planning and statistical modeling, with interlocking and interconnected networks among the various utility companies, electricity is there, with rare exception, when and where you need it. Seamlessly, dynamically responding with as much or as little as you need, on demand.

You buy a sophisticated set top/game console for your entertainment center. You can watch television programming, rent movies on demand, play games locally or even across the Internet. It doesn't hold any content. The content arrives, on demand, through signals sent to an array of virtual servers and processors, from a diverse set of program platforms, publishers and providers. In fact, you are so tech savvy, you even have a locally secure and encrypted Wi-Fi network in your home so you can stream the music, video, gaming and programming content anywhere you put a device capable of receiving the signal, and displaying or playing the content in response to the command of your remote control.

You have no idea where the player that displays *Gone With the Wind* is located, nor do you know where the servers are that connect you, in Minnesota, to gamers in Argentina, France, Thailand and Australia. You can watch broadcast network television, cable, or satellite, or stream music from a variety of sources and access the Internet, right from your living room – or any room. You don't worry about who owns the content or how it happens that when you want content, you can access it with the press of a button or the click of a mouse. Virtual, on-demand service: what, how, when, and wherever you want it. But you do pay a subscription fee, a license fee, or an on-demand fee, or some combination of these, to obtain and use the content.

Now add to these analogies the notion that large-scale digital storage has become increasingly inexpensive. The speed, capacity and ubiquitous availability of high-speed Internet access is already commonplace in many countries and developing

in others, while processors connected to the Internet independent of time zones or geography can move and process digital bits of information and programming at speeds and in a manner inconceivable less than a decade ago.

Now your information and data (your content) can reside in a cloud – virtual storage independent of any one particular server and potentially spread across many. The applications you need, whether you need them daily or once every month, and whether very simple or extraordinarily complex, will likely reside in such a cloud too. You can access them, share them, communicate with others, use, process and manipulate, collaborate, edit and display material anywhere—just plug in, enter your unique user ID and password combination, and it's there, at the press of a button, and the click of a mouse.

Add to this the growing functionality of mobile and wireless devices, and you begin to get a glimpse of the future of cloud computing. You will no longer be tethered either to location or cumbersome devices. Indeed, you can use yours or anyone else's portable input/output device—think Smartphone, netbook, touchpad and more. The programs you need, the data you have created or stored, the communications capability you need are all there in the cloud. Devices will not require increasing processing or battery draining capability, it's all in the cloud. Indeed, most "apps" represent links to data or services, or both, that are accessed but not necessarily stored or processed on the devices themselves. The inevitable reality we're already beginning to witness is that a device equals access—a key that unlocks the wealth of information and processing power that lies beyond. Log in and get started. It will be that simple. Data synchronized and updated in real time. Programs patched, enhanced, updated without the need to distribute, license, download or install. The cloud does that.

Of course, while every cloud has a silver lining, clouds have a dark side as well. Our Cloud Computing Task Force at Reed Smith has created this series of white papers—collectively entitled "Transcending the Cloud: A Legal Guide to the Risks and Rewards of Cloud Computing" to tackle both the opportunities and the dangers; the risks and the rewards. We will try to approach the legal issues and implications a little differently. While much that has already been written about cloud computing concerns itself with data protection, privacy and security—and we will address them as well in what we believe will be a more global and comprehensive manner—our collection of white papers will cover cloud computing issues you may have heard little about, but that are and will be no less significant.

Cloud computing promises great advances in the use of technology by individuals, restoring the power of individually driven communication, creation, collaboration and distribution both to and from individuals, no longer constrained by the need for expensive devices and complex connections. The consumer, the employee, the gamer, the student, will have individualized access to tools and capabilities unheard of even by today's standards. That said, if you can't get to the Internet, or if current bandwidth is strained and unable to carry the traffic, you could be tapping your toes in frustration, waiting while an important document or the collaboration over a file is waiting! While we migrate and evolve, will we still need backup on our devices and, if so, doesn't that defeat the whole purpose? Or can contracts, service levels, requirements and agreements protect you? Do you have insurance to cover these situations? Does your provider? The cloud revolution will create new capabilities, new opportunities, new challenges and new providers seeking to fill those needs. Cloud computing will also create new economic and business models, as well as new economies of scale.

I believe cloud providers will figure out security standards, and while no data protection scheme will ever be perfect, so much has been written and voiced about the issue, it would be hard to imagine that this, along with simply building the necessary infrastructure, is not at the top of the agenda. But because cloud computing is really more a business and process model, not a technological innovation, there are a host of issues that are arising and will continue to arise from this dynamic shift in business processes emanating from cloud computing.

Is a public cloud sufficient for your business or do you need a private cloud—or both (a/k/a, the hybrid cloud), depending on the particular requirement? Corporate technology spending will move from capital equipment or licensing to subscription, usage or demand-based pricing, much like a utility, but possibly segmented by complexity of application, intensity of storage and retrieval requirements, and driven by capacity during peak rather than weak usage periods. What about cloud service providers? We will worry about performance, recovery, and security, as well as availability, which brings us to two points little spoken about these days among the legal community: standards and interoperability.

Electricity and electrical outlets are almost uniform, but not quite. We still carry adaptors and worry about voltage differences across continents and countries. No one cloud provider will be exactly the same as any other, and no single provider is likely to be able to be all things to all customers, everywhere, all the time. But there are currently no standards or any interoperability

requirements, at least nothing binding or even accepted on an industry-wide level. I can call from my mobile phone to any other phone in the world – standards, interconnectivity and interoperability built over years of regulation, consumer and commercial demand make that possible. No such standards and no such interconnection requirements exist in the clouds today. Not only will this pose a challenge to commercial customers and users, but it may also result in barriers to entry among cloud providers—after all, infrastructure is expensive and global capability more so. An antitrust issue? Perhaps. Application developers will compete for cloud apps—remember when word processing programs weren't compatible?

As part of our Cloud Computing initiative, we'll tackle tax and government contracts, antitrust and competition law, and service levels, and we'll give you some insight into our thoughts about e-discovery, litigation and the challenges you will face when a cloud houses your information, and servers are in remote corners of the world and thereby subject to subpoenas in far-reaching and foreign jurisdictions. We'll try to give you some insights by topic—insurance, contract law and regulatory compliance—and we'll try to cover the globe—with papers not only dealing with U.S. law, but from regions and countries around the world as well. Then we'll test what you've learned with case studies. Insights from the same lawyers and professionals who author our white papers will share experience, thought leadership, and helpful hints from the real or potential battlefields. What you need to consider. What you need to know.

Our initiative is not static. Transcending the Cloud will evolve and dynamically provide insights as the industry and the challenges grow. No introduction to our initiative would be complete without thanking the large and growing group of legal professionals here at Reed Smith who took the time to ponder and research and provide you with what would otherwise amount to thousands of dollars of legal work. While each white paper will list the names of the contributors—and I urge you to call upon them directly if a chord (or a nerve) is struck as you read through them. We hope the materials will be insightful, helpful and contribute to the dialog. We will post them on our website (www.ReedSmith.com) and on my blog (www.LegalBytes.com).

As Cloud Computing continues to take shape, answers to unanswered legal questions will begin to unfold—while inevitably new questions will arise. Perhaps in some cases, questions will linger, shrouded in a fog of uncertainty. Our goal, admittedly ambitious, is to stimulate your thinking, have you share with us your concerns, and retain us to help navigate legal issues that may affect you, as we embark on our flight through the clouds. We invite you to be part of our community.

Sincerely,

Joseph I. ("Joe") Rosenbaum
Chair, Advertising Technology & Media Law Practice
+1 212 702.1303
jrosenbaum@reedsmith.com
www.LegalBytes.com

— CHAPTER 1 —

Cloud Computing – The Key Risks and Rewards for Federal Government Contractors

Chapter Authors

Lorraine Mullings Campos, Partner – lcampos@reedsmith.com

Stephanie E. Giese, Associate – sgiese@reedsmith.com

Joelle E.K. Laszlo, Associate – jlaszlo@reedsmith.com

Whether or not you believe cloud computing represents a revolutionary change in the provision of software and data processing services, the cloud and its lexicon have become firm fixtures in corporate enterprise management and, more recently, in doing business with the federal government. As discussed further below, contractors should recognize the legal risks and rewards of both assisting federal agencies in implementing clouds, and in employing cloud service providers to perform federal government contracts.

President Obama's Federal Cloud Computing Initiative

With the release of President Obama's budget for fiscal year 2011,[3] cloud computing also became an essential aspect of the nation's information technology strategy.[4] In fact, the administration has had its eyes on the clouds for some time, and while the 2011 budget represents its strongest commitment toward cloud computing, efforts to implement the concept have been ongoing since at least the roll-out of the 2010 budget.[5]

Around that time, Federal Chief Information Officer ("CIO") Vivek Kundra, the CIO Council, and the Office of Management and Budget established the Federal Cloud Computing Initiative (the "Initiative") to develop a broad strategy and to begin to identify specific applications for cloud computing across the federal government. From the Initiative sprung cross-agency bodies, including the Cloud Computing Executive Steering Committee and the Cloud Computing Advisory Council, and individual agency-based committees like the General Services Administration's ("GSA") Cloud Computing Program Management Office ("CC PMO"). The analysis that follows considers the implementation of cloud computing at the individual agency level, since it is the most immediate, and ultimately the most likely, source of government contracting activity.

Though one of the ultimate goals of the Initiative is to determine whether clouds will provide an appropriate means for breaking down inter-agency data stovepipes, federal cloud computing encompasses four different deployment models, and in these preliminary stages of cloud development, agencies have been free to determine which model best serves their needs. The four models, as defined by the National Institute of Standards and Technology ("NIST"), include: (1) *private clouds*, for the use of a single agency; (2) *community clouds*, shared by multiple agencies; (3) *public clouds*, largely for the public's use and benefit; and (4) *hybrid clouds*, facilitating the sharing of data and utilities across two or more unique clouds of any type.[6] In the sections that follow, we analyze some of the specific legal issues that may arise in the course of government contracting, first in the context of a hybrid cloud, then in the context of a private cloud, and finally in the context of a public cloud. In addressing *hybrid* and *private* cloud computing below, we focus on the key issues contractors should be aware of when assisting federal agencies in implementing cloud computing. In addressing *public* cloud computing, we focus on the key issues that arise when a contractor uses cloud computing to perform its federal government contract.

Key Issues Impacting Contractors Assisting Federal Agencies in Implementing Cloud Computing

Legal Issues in Hybrid Cloud Contracting: GSA's Apps.gov

In September 2009, federal CIO Kundra announced GSA's Apps.gov, which he described as an "online storefront for federal agencies to quickly browse and purchase cloud-based IT services, for productivity, collaboration, and efficiency."[7] Spearheaded by the CC PMO, Apps.gov provides agency consumers four different kinds of cloud computing applications: (1) *business applications*, to facilitate process and analytical tasks; (2) *productivity applications*, to support individual and group functionality; (3) *cloud IT services*, for storing and enabling diverse access to data; and (4) *social media applications*, to enhance communication and collaboration.[8] Again following the NIST taxonomy, the capabilities embodied by the applications on Apps.gov may be delivered to agency customers in one of three methods: (1) *software as a service* ("SaaS"); (2) *platform as a service* ("PaaS"); or (3) *infrastructure as a service* ("IaaS").[9] Perhaps not surprisingly, the delivery method is closely tied to the model of cloud used to provide a particular capability,[10] and a company seeking to offer a particular cloud computing application through Apps.gov will face unique legal implications, based on the method and model involved.[11]

Legal Issues in Contracts Involving SaaS Applications

Business and productivity applications are considered SaaS applications on Apps.gov, and are currently offered mostly through private clouds (though this is an ideal area for the future development of community clouds). Any such application procured through the traditional contracting approach must be certified and accredited by the Federal Information Security Management Agency ("FISMA"). That Certification and Accreditation ("C&A") process, which is defined in the NIST Special Publication ("SP") 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,"[12] is not a prerequisite to being listed as a vendor of SaaS applications through Apps.gov.[13] However, contractors offering these services through Apps.gov must be prepared to work with agency contracting authorities to ensure the C&A process is completed before contract performance begins. Failure to do so may render the contract unenforceable.

Legal Issues in Contracts Involving PaaS and IaaS Applications

PaaS and IaaS applications are not yet available through Apps.gov, though their release is reportedly imminent.[14] These applications will most likely be provided through private clouds in the foreseeable future, and will encompass solutions for data storage, hosting, and processing.

Unlike SaaS providers, IaaS providers will be awarded blanket purchase agreements under their GSA Federal Supply Schedule ("FSS") Schedule 70 contracts, which will implicate different contracting provisions in the Federal Acquisition Regulation ("FAR") from those governing contracts with SaaS providers.[15] In addition, IaaS providers reportedly will be required to meet the "moderate" security level under FISMA standards.[16] The original IaaS request for quotes ("RFQ") that was issued, and later withdrawn in fall 2009, required compliance with Appendices A and B of NIST SP 800-47, "Security Guide for Interconnecting Information Technology Systems."[17] Providers of IaaS capabilities under that RFQ were also held to a guarantee of at least 99.95 percent availability, and agency customers were entitled at any time to complete copies of their own data or the applications through which it was processed.[18] It remains to be seen whether these provisions will be carried into the revised RFQ, but potential providers of PaaS and IaaS capabilities are well advised to brace for stringent data security and access requirements.

Legal Issues Involving the Provision of Social Media Applications

A notable exception to the considerations above applies in the case of free social media applications, including open source, shareware, and freeware tools and services. Since these items are provided free of cost, GSA does not negotiate contracts for their inclusion on Apps.gov.[19] In order to be included as a provider of a social media application on Apps.gov, however, a vendor must agree to abide by a Terms of Service ("TOS") agreement that addresses the particular status and needs of federal government agencies.[20] Working in coordination with several other agencies, GSA developed a model "Federal friendly" TOS agreement[21] meant to serve as a baseline for discussions with individual agency consumers. Prospective providers of social media applications through Apps.gov should review the model TOS carefully, as well as any agency-specific additions or amendments to its terms, to ensure they are able to comply with its provisions.

Legal Issues in Private Cloud Contracting: Department of Defense ("DoD") Initiatives

Rapid Access Computing Environment ("RACE")

Unlike GSA, DoD is currently focused on developing private cloud environments where the data center is controlled by DoD rather than outsourced.[22] DoD expects this approach to achieve the cost savings typical of cloud computing and to address cybersecurity concerns.[23]

One example of a DoD private cloud is the Defense Information Systems Agency ("DISA") Rapid Access Computing Environment. RACE is an internal cloud computing service – a service controlled by DISA in its Defense Enterprise Computing Centers ("DECC") and operated behind DoD firewalls with the support of federal government contractors.[24] Similar to other clouding computing services, DoD users only pay for the amount of storage and processing power they need based on a monthly fee.[25] Within 24 hours of payment, users can begin using the RACE computing resources to develop and test their applications in their own Windows or Red Hat Linux operating environment.[26] When the application goes into production, the resources are returned to the DISA's cloud at one of DECC locations.[27] In the future, RACE may be extended to production of computing processes and applications.[28] In addition to cost savings, RACE offers the potential to standardize software applications across DoD agencies, making collaboration among the agencies easier.[29]

Transitioning Existing IT Systems to Cloud Computing Environments

Beyond supporting new cloud computing environments like RACE, government contractors are assisting DoD agencies with the transition of existing IT systems to cloud computing. For example, the U.S. Navy has awarded Lockheed Martin Corporation and Northrop Grumman Corporation Consolidated Afloat Networks and Enterprise Services ("CANES") contracts totaling $1.75 billion to upgrade existing shipboard and onshore Internet Protocol networks for command, control, communications, computers, intelligence, surveillance and reconnaissance ("C4ISR").[30] Under the CANES contracts, the companies will transition these Navy networks to cloud computing environments.[31]

Legal Issues Associated with Cybersecurity

Whether discussing cloud computing in terms of networks like RACE, where it is inherent, or CANES, where it is being adopted, the same cybersecurity issues apply. Cybersecurity includes safeguarding systems from security breaches, maintaining system operations while a cyber attack is underway, and developing network self-healing capabilities to minimize the impact of cyber assaults. Secretary of Defense Robert Gates has stated the United States is "under cyberattack virtually all the time, every day," and cybersecurity is not a new issue for DoD.[32] Of course, some cyberattacks are more damaging to national security than others. In a series of cyberattacks attributed to the Chinese government, computer hackers recently stole several terabytes of technical specifications pertaining to the Pentagon's $300 billion F-35 Joint Strike Fighter development program, and to the Air Force's air traffic control system.[33]

Given these kinds of cyber threats, federal government contractors implementing cloud computing technologies for DoD should expect compliance requirements related to cybersecurity to continue to evolve. Today, DoD contractors must comply with the Defense Information Assurance Certification and Accreditation Process ("DIACAP") when such requirements are included in their contracts.[34] Federal contractors required to seek C&A under DIACAP should recognize that this can be a lengthy, expensive process.[35] In addition to DIACAP, DoD contractors can expect new regulations to be promulgated related to cybersecurity. For example, Federal Desktop Core Configuration ("FDCC") security setting requirements may be incorporated into the FAR to standardize the FDCC contract clauses federal agencies are already required to include in their IT contracts.[36] Because these kinds of requirements will continue to evolve, Federal government contractors should carefully analyze the cybersecurity specifications in their DoD contracts.

Key Issues Impacting Contractors Using Cloud Computing in the Performance of Federal Government Contracts

Public Cloud Services Employed by Federal Government Contractors

Federal government contractors already use public cloud computing services to carry out their contracts. For example, cloud service providers offer applications and computing power to enable federal contractors to manage and collaborate on government projects in real-time, as well as to automate business processes such as those for timekeeping and compliance with federal fiscal requirements, such as earned value management.[37] Government contractors using these services expect to achieve greater efficiencies through collaborative online project management and increased visibility into project health.[38]

Government contractors are also hiring cloud service providers that offer "FAR compliant accounting platforms that can satisfy audit requirements of the Defense Contract Audit Agency ("DCAA")."[39] Here small and medium-sized government contractors expect to reduce the cost of compliance with federal government accounting regulations by avoiding the cost of implementing and maintaining such compliance systems in-house, and instead paying commercial cloud providers a less costly usage fee to store, accumulate, and report accounting data in compliance with the FAR.[40] These cloud service providers typically promise a government contractor a certain level of security, as well as 24-hour-a-day, on-demand access to data and applications stored in the cloud.

Cloud Service Providers as Federal Government Subcontractors

A government prime contractor may need to treat its cloud service provider like a government subcontractor when the services, such as those discussed above, are required to perform a federal government contract. This raises several legal issues that government prime contractors should consider carefully to avoid potential administrative, civil or criminal liability. As discussed further below, to mitigate the prime contractor's potential liability, the prime contractor, more often than not, will need to negotiate contract terms with the cloud service provider that the provider would typically not accept from its other commercial customers.

Legal Issues Arising from Government Information Assurance and Security Requirements

Depending on the federal government's view of the criticality or confidentiality of the data maintained by the cloud service provider, a government prime contractor may need to include in its contract with the cloud service provider certain federally mandated information assurance or security requirements. For example, the prime contactor and its cloud service provider may be required to comply with the DIACAP or the NIST C&A standards discussed above. Further, the prime contractor and the cloud provider may be required to allow government inspection of the privacy and security safeguards at their respective facilities, and to notify the government of any failure of those safeguards.[41] In addition, under certain circumstances, the government may require the prime contractor to maintain a continuity-of-operations plan in the event of a catastrophic failure of the primary information systems. In order to execute that plan, the prime contractor may need to contractually impose certain requirements on the cloud service provider. Thus, in order to comply with information assurance and security requirements pursuant to its contract with the government, the prime contractor may need to flow down these same requirements in its contract with the cloud service provider.

Legal Issues Arising from Government Business Practice Requirements

The prime contractor also may need to flow down to the cloud service provider certain government compliance requirements related to business practices in its prime contract. For example, during certain DCAA audits, the government will evaluate the adequacy of the prime contractor's systems, policies, procedures and internal controls related to the performance of its government contracts.[42] If the cloud service provider is operating an internal control system for the prime contractor, such as storing, accumulating and reporting the prime contractor's accounting data in compliance with the FAR, the prime contractor must ensure the cloud service provider is contractually bound to comply with the federal government requirements applicable to the prime contractor, as well as the prime contractor's policies and procedures. If providing cloud-based services for processing the prime contractor's accounting data, the cloud service provider may also be required to comply with the federal government's Cost Principles and Cost Accounting Standards.[43] If the prime contractor does not require the cloud service provider to comply with federal government requirements applicable to the prime contractor, the prime contractor may suffer the consequences of failing a government audit.

Additionally, prime contractors are required to comply with certain document retention requirements under the FAR.[44] A prime contractor should ensure that its cloud service provider's retention policies do not conflict with the FAR requirements, because, among other reasons, the prime contractor needs its data maintained in accordance with the FAR and readily available in the event of a government audit. The case study below provides an illustration of some of this and other potential legal risks, as well as the rewards, of employing a cloud service provider in performing a federal government contract.

Case Study: The Risks and Rewards of a U.S. Federal Government Contractor Employing a Cloud Service Provider to Perform a Federal Government Contract

By way of illustrating the importance of addressing the specific legal implications that arise in the context of government contracts whose performance involves the use of cloud computing, we offer the following hypothetical situation: a Small Business Administration-certified 8(a) staffing company, SB, teams with a joint venture partner, JV, to compete for, and ultimately win, a three-year U.S. Army contract for the provision of medical personnel at various military hospitals and clinics across the country. While SB and JV have performed similar contracts in the past to provide health research and practitioner staff to civilian government agencies, the Army contract represents a new foray into military contracting for both partners. While both partners are aware that the Defense Contracting Audit Agency ("DCAA") will audit the contractors' accounting systems for compliance with the Federal accounting regulations, including the Federal Cost Accounting Standards which are applicable to the joint venture under this contract, neither partner is sure of what is required to comply with those regulations, or how their current systems measure up.

The Rewards of Cloud Computing

Because the Army contract represents an entirely new line of business for SB and JV, and one they are not sure they will continue after completion of the contract, neither is quite ready to assume the expense and complexity involved in adopting new accounting systems that comply with Federal accounting regulations. Thus, SB and JV decide to outsource all of the accounting tasks associated with the Army contract to a mid-sized firm, MF, that has recently announced a new cloud-based accounting service that complies with the FAR ("Federal Acquisition Regulation"). The terms of the Army contract do not prohibit this kind of subcontracting, but the contract also does not explicitly specify terms & conditions related to data retention under the FAR that should be flowed down to such a contractor. Further, the prime contractor fails to flow down these FAR requirements to the cloud computing service provider.

The Risks of Cloud Computing

The contract, to all outside observers, is successfully performed by SB and JV. In fact, all is well, until just under two years after the contract is completed and final payment has been made. At this point, a woman who worked as a dental hygienist under the contract alleges that irregularities in the electronic timecard system employed by SB and JV led it knowingly to submit false invoices to the Army, and thereby violate the False Claims Act. The Government intervenes and DCAA immediately initiates an audit of the completed contract. Unfortunately, though DCAA found MF's accounting system complied with Federal accounting regulations during performance of the contract, MF failed to maintain the accounting data for the period of time required by the FAR after the contract was completed. Many of the records no longer available include accounting data from the Army contract, the production of which DCAA now demands. Thus, the prime contractor no longer has the accounting data it was required to maintain under the FAR to support costs it billed to the Army. As a result, the prime contractor will have greater difficulty refuting the alleged false claim to the Army.

Mitigating the Risk

This scenario demonstrates the importance of structuring the prime contractor-subcontractor relationship in light of the Federal government's right to audit the performance of a contract. This is particularly true where the prime contractor decides to subcontract the task of managing data essential to the contract's performance (and therefore relevant to any potential audit). When the subcontractor provides its services through cloud computing, even if the prime-subcontractor agreement mandates near-constant availability of the data, the prime contractor must take care to ensure that the particular requirements for data maintenance imposed by the FAR are flowed down to the subcontractor. As added protection, the prime contractor may also seek a contract clause providing that the subcontractor will indemnify the prime contractor for liability that arises in the event that the subcontractor fails to maintain the data as specified in the prime-subcontractor arrangement. From the subcontractor's perspective, it is equally important to understand the terms of the arrangement, particularly the responsibility it imposes on the subcontractor to provide a certain level of data and services, and exactly what that level is. A cloud computing subcontractor who agrees to indemnify the prime contractor in the event that essential data is lost or inaccessible may choose to build the cost of this provision, or the cost of undertaking insurance for such a contingency, into its price to the prime contractor.

What You Should Do

Like other technology-related developments of the past hundred years, cloud computing poses benefits and risks for Federal government contractors. But failing to recognize the unique legal implications of cloud computing presented by each Federal contracting opportunity, and to carry on with business as usual, could expose a contractor to potentially significant liability. Federal government contractors should work with legal counsel to identify and mitigate those risks, including starting early in the contracting process with the negotiation of terms and conditions of the prime contract and any related subcontracts. By mitigating those risks, a Federal government contractor paves the way for using the cloud to revolutionize how it does business with the Federal government.

— CHAPTER 2 —

Pennies From Heaven – U.S. State Tax Implications Within Cloud Computing

Chapter Authors

Michael A. Jacobs, Partner – mjacobs@reedsmith.com

Kelley C. Miller, Associate – kmiller@reedsmith.com

Introduction—The Landscape

Faced with growing budget deficits and decreasing tax bases, some states in the United States are searching for new and broader avenues for revenue generation. Digital products and electronic commerce are two of the most notable, recent targets in the states' search for revenue. Just as many states have begun to expand their sales-tax laws to reach digital products, such as music, software, and audio-visual downloads, the cloud computing phenomenon, and the shift from downloaded products to Internet-based access to applications and data "in the cloud," has the potential to once again take a large segment of digital transactions outside of the states' taxing reach. At the very least, cloud computing promises to raise a series of new questions, the most basic of which is how states will presumably impose sales tax on digital transactions.

Currently, 46[45] U.S. states impose some sort of sales tax, at least 12 states impose a sales tax on digital goods, and another 17 states are likely to consider legislation to impose a sales tax on digital transactions this year. Thus, sales-tax issues are likely to be a significant concern not just for cloud computing vendors, but also for most consumers of cloud computing services with U.S. operations.

Taxing Digital Transactions—Sales Tax Implications for Cloud Computing Vendors

Historically, state sales taxes were taxes imposed on sales of tangible personal property, and a few specified services. However, as the U.S. economy has evolved, states have moved to expand their sales-tax bases to include more services, as well as digital products and transactions.

Some states have enacted legislation imposing sales tax on specific digital transactions, such as music downloads, either through an expansion of the definition of tangible personal property, or through the creation of a new class of taxable transactions. The rationale behind this legislation has been to ensure that, as consumers substitute purchases of digital products for their tangible counterparts, state sales-tax bases do not continue to erode.

Recently, and perhaps with the emergence of new digital technologies like cloud computing in mind, some states (*e.g.*, Kentucky, North Carolina, Washington, and Wisconsin) have expanded their sales-tax laws even further, by enacting provisions that tax digital products with service-like characteristics, such as access to data and data processing[46]. Notably, Washington imposes sales tax on digital services, which is broadly defined to include a "service that is transferred electronically that uses one or more software applications."[47] This expansion of state sales-tax bases to encompass "digital services" is evidence that states are gaining awareness of the Internet-based nature of cloud computing. This development also crystallizes an important state sales-tax question for cloud computing vendors—namely, what components of cloud computing pose state tax implications?

Pinning Down the Clouds

The key issues in applying state sales-tax laws to cloud computing are: (i) nexus (does a cloud computing transaction have sufficient contacts with a state in order to allow the state to impose sales tax on the transaction?); (ii) taxability (are cloud computing transactions products or services of a type that are subject to state sales tax?); and (iii) sourcing (which state (or states) can tax a particular cloud computing transaction?). Each of these questions is addressed below.

The answers to these questions vary by state, and are neither definite nor consistent. For example, for purposes of determining taxability, some states may view a cloud computing transaction as the provision of a taxable computing service. Other states may characterize a cloud computing transaction as a series of distinct transactions—each with its own sales-tax treatment. Thus, a state could characterize a cloud computing transaction as the provision of computing services, coupled with a lease of server space, and the sale of a software product.

Nexus

Before the complex issues of taxability and sourcing can be addressed, a vendor of cloud computing services must first consider the threshold issue of nexus. "Nexus" is the term used to describe the amount and degree of business activity that an entity must have in a state before the state can subject the entity to state tax. Nexus determinations tend to be highly fact-specific, and rely on an application of a complex mix of U.S. constitutional and state statutory law. Cloud computing adds another layer of complexity to the determination of whether sufficient contacts exist to create nexus for sales-tax purposes. If a transaction occurs "in the cloud," does the transaction have sufficient contacts with any state to allow the state to pull the cloud, and its users, down to earth (*i.e.*, establish nexus)?

Although at this time there is no definitive answer to the question of how the concept of sales-tax nexus applies to a cloud computing transaction, there is a base of authority to guide taxpayers, states, and the judiciary as cloud computing becomes the norm. In the 1992 case of *Quill Corp. v. North Dakota*, 504 U.S. 298 (1992), the court ruled that before a state could impose a sales-tax collection obligation on an entity, the Commerce Clause of the U.S. Constitution required the entity to have a "substantial nexus" with the state, as indicated by physical presence. Since *Quill*, the challenge has been to determine how much and which type of physical presence is sufficient to satisfy *Quill*'s requirement of "substantial nexus."

In the case of cloud computing service providers, questions are likely to arise regarding whether a vendor providing cloud computing services to a customer in a state has sufficient nexus with that state to be required to collect the state's sales tax. In order to satisfy the "substantial nexus" requirement, must a vendor own or use servers located in the state? Or is it sufficient that the vendor is licensing software to customers in the state and a portion of the software resides, at least temporarily, on the customer's computer located in the state? Although a handful of states have provided a legislative safe harbor for presence of data on servers located within those states, the United States Supreme Court has yet to revisit its decision in *Quill* as to whether the mere presence of electronic data is a physical presence sufficient to establish nexus. Accordingly, the elements of and issues inherent to the taxability of cloud computing transactions are currently being addressed on a state-by-state basis.

Taxability of Services, Leases, and APIs

A cloud computing transaction typically involves providing a consumer with a combination of an Internet-based hosting platform, support for programming languages, disk space, a back-end database, and bandwidth. The signature characteristic of cloud computing is that it allows a consumer to simultaneously engage servers, storage, and bandwidth on an "as needed" basis. The result is that the customer may be consuming services (computer and data services) and space, while simultaneously purchasing applications and the right to access data (lease of server space). Additionally, there is a plethora of cloud computing types. For example, cloud computing vendors may offer: increased computing power or storage space (infrastructure); a platform on which providers may develop and access specific applications (service and data platforms); and customer-specific software development and hosting. With respect to the latter, a customer-specific application may be created that can be constantly updated and manipulated to interface with a vendor's database. An application program interface (API) then allows the customer-specific application to interact with the API, often across multiple servers. In sum, cloud computing transactions may be described as a web of interactions between vendor and consumer, involving multiple, simultaneous exchanges of services and products occurring in numerous locations.

From a state tax perspective, this web of interactions presents many issues, the most significant of which are:

- How will a state elect to impose sales tax on a cloud computing transaction that bundles together the sale of services, with access to server or disk space (which would likely be structured through a lease), and the ability to interface with vendor applications? Each of these services or products would typically be afforded very disparate state tax treatment if sold separately.
- How will a state elect to tax customer-created applications that interact with its database? Will these applications be deemed to be akin to custom software, which is exempt in many states?

While it is unclear as to how the states will address the taxation of cloud computing, there is some indication as to the direction in which some states are heading. The Washington tax referenced above on digital services is a key example. By encompassing a broad range of digital services, including those that utilize software applications—the very essence of cloud computing—Washington's tax on digital services is evidence of one state adopting a very broad approach to bundle the elements of cloud computing into a single taxable transaction.

Outside of the cloud computing context, some states tax transactions that involve the provision of a combination of taxable and non-taxable goods and/or services by looking to the essence of such "bundled" transactions. In contrast, other states have taken the position that if a bundled transaction involves the provision of more than a de minimis amount of taxable goods or services, then the entire transaction is taxed. The states that have opted for this "all or nothing" approach to bundled transactions will likely opt to treat cloud computing transactions as taxable in their entirety, regardless of any elements that might be nontaxable if provided separately. However, other states may allow vendors to bifurcate cloud computing transactions between taxable elements (such as generic or non-custom applications and data services) and exempt products (like access services, custom-applications, and leases of server space, dependent, of course, on whether there is nexus.

Sourcing

While the characterization of cloud computing components as taxable or nontaxable is an essential part of understanding the state tax implications of cloud computing, it is the first level of a two-part inquiry. Both the characterization and the source of the taxable commodity must be determined in order to understand the overall state tax implications of a transaction. The second part of the inquiry—sourcing—is important in cloud computing because it determines which state may tax a particular transaction. The states use two traditional methods for sourcing transactions for sales-tax purposes: origin- and destination-based sourcing. Under the origin-sourcing method, a transaction is generally taxed by the jurisdiction where the taxable service or product originates, while under the destination-sourcing method, a transaction is generally taxed by the jurisdiction where the taxable service or product is consumed. Currently, most states use a destination-based sourcing.

Cloud computing raises a multitude of novel sourcing issues for states using both the origin- and destination-sourcing methods. For example, in the minority of states that use the origin-sourcing method (*e.g.*, Arizona, California, Illinois, Mississippi, Missouri, New Mexico, Pennsylvania, Tennessee, Texas, Utah, and Virginia), the sourcing of cloud computing services will raise complex issues because the very nature of cloud computing may make it difficult, if not impossible, to attribute the origin of the service to any one jurisdiction. Even for those states that employ destination-based sourcing, the flexible and interactive nature of cloud computing presents unresolved issues. For example, what is the destination of a cloud computing transaction in which a consumer accesses multiple vendor servers with no discernable location, or if applications are created and data is accessed and stored for the consumer's use on multiple servers? Overall, the true hallmark of cloud computing—the ability for vendors and consumers alike to access and interact with a completely Internet-based scheme—obviates the ability to determine where the consumer is located and where it is using the objects of cloud computing.

Metering

One unique and potentially helpful characteristic of cloud computing from a state sales-tax perspective is that cloud computing services can be (and often are) sold on a metered basis. Thus, cloud computing vendors typically charge customers only for actual use of bandwidth computing time, and disk space. This metering may allow the various components of a total cloud computing transaction to be itemized into discrete charges. From a sales-tax perspective, metering may allow some vendors to itemize their charges in such a manner that their invoices show separate charges for the taxable and non-taxable portions of a cloud computing service. However, not all cloud computing vendors are currently selling their services on a metered basis. Instead, many vendors treat cloud computing as a bundled transaction, and invoice customers a single charge for what may otherwise be a combination of taxable and exempt components.

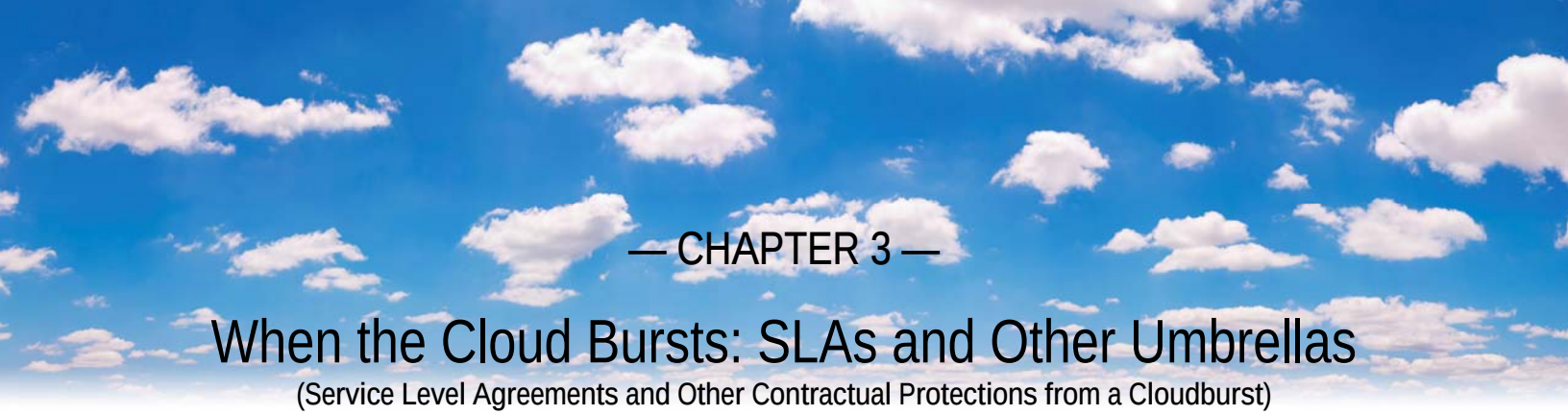
Summary of Essential State Tax Considerations

In summary, cloud computing raises numerous and unresolved state sales-tax issues. These issues are likely to be resolved piecemeal on a state-by-state basis. However, as they are being resolved, cloud computing will present vendors and consumers with potential sales-tax planning opportunities. In many cases, cloud computing will make it possible for consumers to obtain many of the benefits that were once associated with taxable purchases

of software and digital products, through the purchase of a nontaxable service. In addition, because of the uncertainties regarding the sourcing of cloud computing transactions, vendors and consumers may have opportunities to achieve more advantageous sourcing for transactions by moving them to the cloud. For instance, there may be opportunities to move data processing services from origin-sourcing states that tax such services, to the cloud.

However, to take advantage of these opportunities, and to avoid pitfalls, cloud computing vendors and consumers will need to focus on the following factors:

- In what state is the cloud computing vendor located? In what state is the consumer and its server(s) located?
- Does the cloud computing vendor have nexus in the state where the customer is located? Where are the vendor's server(s) located? Are certain servers (or server space) "fixed" and dedicated for specific consumers?
- What type of cloud computing is being provided (computer or data service, server space, software applications)? Is there a primary component?
- With respect to applications, are the applications created specifically for the consumer? Does the consumer receive a copy of or have access to the application outside of any interface with the vendor's API?
- Who is "using" the application created for the consumer? Is the vendor using the software application to provide a service to the consumer, or is the vendor licensing the software application to the consumer for its use?
- How are the provision of data processing or computer services and the provision of software taxed (characterization and sourcing rules) in the states where the vendor, consumer and server(s) are located?



— CHAPTER 3 —

When the Cloud Bursts: SLAs and Other Umbrellas

(Service Level Agreements and Other Contractual Protections from a Cloudburst)

Chapter Author

Rauer L. Meyer, Partner – rlmeyer@reedsmith.com

New Benefits, New Risks

Cloud computing is increasingly becoming an appealing method of obtaining computing services, as it offers both dramatically lower costs and scalability, which in turn are the result of features that are inherently double-edged. Among the realities that customers/users of cloud computing must reconcile are:

- Their data, applications and infrastructure are stored and managed by others in remote locations
- Their proprietary data can be stored with the data of other tenants (some of whom may even be competitors) on shared infrastructure (at least in the public cloud)
- Access and use is through the Internet, and hence, depends on its bandwidth and availability
- Hosting facilities are often sited in low-cost locations with cheap power
- Cloud computing providers often subcontract and outsource the provisioning of their services to unknown third parties in unknown locations

New Risks, New Concerns

As customers and providers alike now begin to realize the benefits offered through cloud computing, they must also face a series of new risks and fears. Granted, while some of these concerns existed prior to the onset of cloud computing in the context of third-party services, many are most definitely new. The following is just a sampling of these risks:

- Loss of service as a result of provider outages. There have been several well publicized cases recently in which customer data was lost. In fall 2009, a server-failure affected some of T-Mobile's Sidekick customers, resulting in the loss of considerable contact and calendar data. Google Apps has been down on several occasions over the past couple years for several hours at a time, obviously impacting business customers. Amazon S3 was down for almost an entire day in 2008. Back in September 2009, Workday, a provider of human resource, financial, and payroll applications, suffered a 15-hour outage and had to resort to a long backup data center transition.
- Slow performance and response times because of connectivity and bandwidth problems and insufficiencies
- Loss of data privacy and security breaches. Many surveys of information technology and data processing professionals have put this concern atop the list, even ahead of performance, provider financial liability and business continuity.
- Ineffective/inadequate disaster recovery. With many small and mid-size cloud computing providers opting to establish facilities and infrastructure in countries that offer less expensive power and utility resources, more favorable tax laws, and often less stringent business and labor laws and regulations, onsite expertise and oversight may be minimal. Hence, when the cloud goes down, those customers with critical data at risk may not get the fixes, attention and information they need to effectively manage the situation.
- Uncertain regulatory compliance. Although customers in regulated industries (*i.e.*, financial services, health care, broker/dealer, etc.) have the same desire to migrate their networks and systems to a cloud environment for all the benefits available to them via cloud computing, they must be acutely aware of the unique set of risks that other customers in non-regulated industries may not necessarily face. By its

distributed nature, cloud computing often blurs the location of and security measures associated with data. These customers or their advisors must be familiar enough with the regulations that govern their business in order to assess the viability and risk levels of putting their data, network services and processing into the cloud.

General Risk Mitigation

As described above, cloud computing can pose potentially serious risks to customers. Thus, how can they reap the benefits of the cloud while minimizing the risks? Cloud computing needs effective and credible risk management, and remedies for failures. Information technology and data processing professionals recommend several approaches to avoid bad outcomes, among them: Recognize that some things may not belong in the cloud (or at least a public cloud) in the first place, such as critical business data, legacy enterprise applications, ERP, personal data, and highly transactional systems or latency-sensitive data. Customers should think twice before moving critical data into the cloud without an effective backup plan.

- Plan a good mix of public, private, and hybrid clouds[48], depending on a customer's risk analysis.
- Conduct a reasonably thorough due diligence of the cloud computing providers being considered. Get references and talk to existing customers. Seek to conduct pilot tests of the provider's system.
- Establish one's own disaster recovery and backup capabilities for anything sent to the cloud, thereby not relying exclusively on the cloud provider.
- Reserve the right and establish a mechanism for the customer to terminate its cloud computing agreement, and confirm (i) one's ability to retrieve its data from the cloud (don't take this for granted), and (ii) one's right to transition from the provider's cloud to another service or to its own data center.

But for all these measures and precautions, bad outcomes may still happen. Accordingly, the customer owes it to itself to be proactive and seek out the best remedy available to it in the service contract—if the cloud should burst.

The SLA Solution

The service level agreement (SLA) part of contracts between providers and customers is a familiar part of almost every computing or information processing service arrangement. In cloud computing, while the SLA serves similar purposes, it requires some adaptation to the new risks of the cloud, and its benefits should get a fresh evaluation in the overall risk management analysis.

Service providers typically offer SLAs as a limited remedy for their customers for failures in the provider's own systems. An SLA specifies service level metrics (*e.g.*, system uptime of 99.99 percent each month, average help desk service response time of 15 minutes). The provider's actual performance is monitored, measured against the standards, and reported to the customer. Substandard performance triggers credits against fees or services, in the nature of liquidated damages, within limits that the provider can live with, especially if (as is usual) many customers will be affected by the same failure. Notably, only failures within the provider's control, will trigger the credits. Providers understandably disclaim responsibility for things out of their control such as Internet connectivity. Finally, often (but not always) the provider requires the customer to agree that these credits are the customer's sole and exclusive remedy for the failure. In other words, even if a customer suffers considerably greater losses as a result of some information technology or data processing failure, it's essentially stuck with the credits and the credits alone.

The SLA is supposed to provide a customer with two kinds of protections:

- An incentive for the provider to perform as promised, giving it skin in the game
- Some compensation for the customer's losses from a failure

However, SLAs are increasingly viewed by customers as unsatisfactory forms of protection that weigh heavily in the provider's favor. First and foremost, disputes often arise over the monitoring of performance and fault, especially when the governing records are those of the provider. Also, if the provider's skin in the game is modest and less than its cost to provide better service, it is not much of an incentive. Moreover, the compensation for customer loss is inherently unpredictable, and in those rare instances in which a customer will be compensated for its actual damage through the SLA, it will generally be coincidental. As a result, customer information technology and data processing departments often view SLAs as more trouble than they're worth.

Without an SLA or an equivalent liquidated damage provision, a customer is left to its general contract remedies, which have their own shortcomings. A customer is in theory entitled to recover its entire loss if it can prove that the provider was at fault and in breach. Information

technology and data processing provider contracts invariably disclaim consequential damages (*e.g.*, lost profits) and put a cap on direct damages (*e.g.*, fees paid to the provider). Add to these uncertainties the certain cost and delay of litigation, and it's not a pretty remedy for the customer.

In the current cloud computing market, providers typically promote "reliable service," since this is a common customer concern, and offer SLAs of one variety or another. As an example of current offerings, the SLAs of most providers "guarantee" some uptime metrics ranging from 99.95 percent to even 100 percent availability each month. Amazon EC2 offers 99.95 percent, AT&T Synaptic Hosting offers 99.7 percent, and 3Tera commits to 99.999 percent for a virtual private data center. Many providers offer options at different percentage rates for different prices. But these numbers by themselves translate into small comfort for the customer in the typical case as they measure cumulative downtime (*i.e.*, not per-incident) and their true value turns on the nature and size of the credits. These solutions to the remedy problem will no doubt evolve as customers demand more assurances from cloud providers.

Can cloud computing SLAs even be negotiated? Many public cloud services are available only through non-negotiable click-wrap contracts that cannot be negotiated and strictly limit the provider's liability, since the model is based on a low-cost, one-size-fits-all offering that avoids customization. In this case, the SLA remedy is not worth much. SLAs play a more important role in the private cloud model, where customers can do several things to improve their remedies. Private cloud SLAs are usually negotiable, since the provider is only negotiating with a single user for a single hosting environment, rather than having to guarantee different service levels to different users of the same cloud. The more a customer brings to the provider, such as large upfront fees (*e.g.*, for migration and implementation) or a large volume of services, the more power it will typically have to negotiate. The customer should always try, keeping in mind that better protection will come with higher fees.

Here are some tips a customer should consider:

- Adapt your SLA remedies to your use case. As mentioned above, if you are merely developing a new system that is not overly time- or data-sensitive, you might not need the tightest SLA possible. The provider's standard SLA could very likely suitable. But if a service failure will harm your business significantly, the standard offering will not be enough.
- The basic model of the common SLA is inadequate and should be rethought for cloud service risks. In a given metric (*e.g.*, availability), a single percentage of uptime is specified on a cumulative basis over a month and a single credit is provided if the standard is missed. If it is missed, however, typically a singe credit ($X) or discount is given to the customer against its hosting costs, which constitute the customer's sole remedy. But what if a single outage continues for many multiples of the metric? The customer still gets only its $X, nothing more.

The incentives and compensation in this structure haven't seemed to evolve as quickly as the technological offerings. Customers instead should ask for graduated credits that increase over time with each incident. For example:

Downtime per Incident	Credit
First Hour	$X
Next 2 hours	2$X
Next 2 hours	4$X

By tying the credits to single incidents, the provider is motivated to fix each one and, by increasing the credits over the time of the failure, to fix it quickly. It also better measures and compensates actual loss to the customer. This way, the interests of both provider and customer are better aligned. In return for this more favorable SLA, the customer can more easily accept that these credits will constitute its sole and exclusive remedy for the failure in question.

- Who should be monitoring the provider's performance? The customer should ask that a pre-agreed, third-party, performance-management provider (such as Cloudkick, Gomez, or Apparent Networks) monitor and report provider performance against the SLA's metrics. Many providers will not accept a third-party's measurements when credits are claimed, but even if they do not, a customer is advised to conduct its own monitoring. This, at least, enables the customer to verify the provider's reporting data and detect problems early on, often before the provider takes action.
- The typical information technology and data processing SLA measures availability and customer service response time. The customer should develop additional metrics in a cloud SLA for its own use. If security is critical, the customer should measure

security failures. If scalability is critical, the customer should build a metric to measure this. If a provider uses geographically distributed servers in the cloud to serve a global, broad market, the customer should measure the metrics on a region-by-region basis. And, as always, the provider should provide a periodic report of performance against these metrics.

- Customers are strongly encouraged to facilitate proof of the failures that trigger the credits, and evaluate their own internal risks and likelihood of failure. To the extent practicable, the customer must seek to measure the traffic, bandwidth levels, and connectivity in its own network before expanding to the cloud. If a customer understands the points of failure in its own environment, these can be separately mitigated and also facilitate a cause analysis vis-à-vis the cloud provider in the event of failure. This applies especially to the experience of remote workers who are connecting from home networks.

Conclusion

Like most things in life, cloud computing can very much be a double-edged sword. Further compounding some customers' reluctance to entertain and/or migrate into a cloud environment, most cloud computing contracts to date leave customers much to desire. It is essential, therefore, for a customer to have its cloud computing contract reviewed by competent counsel who is knowledgeable and familiar with his/her client's issues and concerns, the technology and services involved, and industry standards. Again, the goal of any contract (and cloud computing contracts no less) should be to capture a fair, balanced and realistic set of terms that depict the transaction, deter complacency, protect that which is most vulnerable, and incentivize the parties to do their best work at all times. This may not be easy to accomplish in the early days of cloud computing, but whoever said the business of technology should be easy?

— CHAPTER 4 —

E-Discovery and the Cloud: Best Practices in the New Frontier

Chapter Authors

Jennifer Yule DePriest, Partner – jdepriest@reedsmith.com

Claire Covington, Associate – ccovington@reedsmith.com

Introduction

During the past five years or so, lawyers and their clients have struggled to reconcile their discovery obligations under federal and state discovery rules with the ever-expanding digital universe. Indeed, as technology continues to evolve, the *digital sea* of electronically stored information ("ESI") produced by companies continues to rise. Consequently, the costs associated with creating new information technology (or "IT") infrastructure, and with maintaining and preserving (or hosting) ESI, also continue to rise. In many cases, the duality of rising costs and increased technological complexity have led companies to look to third-party providers for some or all of their infrastructure and hosting needs. In fact, third-party hosts and IT service providers of varying sizes and offerings are essentially a ubiquitous reality in our digital economy today. Consequently, it should not be a surprise that cloud computing represents a natural, albeit somewhat different, model in the evolution of the use of IT.

Cloud computing is the term ascribed to the industry shift and transformation from companies either hosting and managing their own applications and data on local servers, or entering into micro-hosting arrangements with third-party providers to a grid computing model in which users access a shared computing environment typically being provided by large and well-entrenched technology companies such as Google, Microsoft, IBM and Amazon. For many companies that have embraced cloud computing for all or some of the IT and hosting needs, gone are the days of purchasing departments ordering server after server and rack after rack, or negotiating co-location agreements in which their servers sit within some third-party's server farm in downtown Toronto, Miami or Seattle. Rather, the cloud is an entirely virtual environment with digital tributaries that span the globe, moving data from one server to another to achieve optimal data storage and retrieval capabilities, bandwidth optimization, and overall IT cost-effectiveness, providing all of a company's data storage, data processing and distribution needs on an as-needed basis (think "utility"). This has already begun to transform the traditional IT model for multinationals, and continuing the trend that began with hosting and outsourcing, will effectively relieve companies of the burden and expense of maintaining their own electronic data and monitoring their own IT infrastructure.[49] While there were good reasons, pre-dating the commercial use of the Internet, that the old timesharing models of the 1960s fell by the wayside and gave way to corporate IT infrastructure development, the environment has changed and cloud computing is an idea whose time may have now arrived.

So, what is it about the new age of discovery and terms like "cloud computing" that leave lawyers (and perhaps some clients) with a great degree of caution? Put simply, it is the existence of a tremendous amount of electronic data, the potential for lack of control over its location and attendant uncertainty about the ability to find and process relevant information in connection with a lawsuit. This fear lies in the fact that for purposes of meeting discovery obligations, a company's data is likely considered to be in the company's *legal* "control," though a third party actually has the data. Also uncertain is what is considered "reasonable" with respect to efforts to identify, preserve and collect relevant information "in the cloud" under the discovery rules.

This paper will briefly discuss discovery obligations under the Federal Rules, specifically with respect to e-discovery[50]; the "reasonableness" standard as it relates to identification, preservation and collection of ESI; and particularly electronic information stored in the cloud. In that regard, this paper will highlight issues to address with your cloud provider that may help you minimize cost and burden, and

help establish "reasonableness" for purposes of meeting your discovery obligations.

Discovery obligations

Discovery involves the identification, preservation, collection, review and production of relevant information in a party's possession, custody or control.[51]

Though living in the digital age may have made certain aspects of modern life much easier—fewer bankers' boxes and paper cuts, for instance—it has undoubtedly made litigation, and discovery in particular, more difficult and costly. So much more difficult, in fact, that the Federal Rules of Civil Procedure were amended in 2006 just to accommodate the rising tide of e discovery in litigation.[52]

The 2006 amendments to the Federal Rules expanded the scope of a party's discovery obligations to account for the increasing amount of business conducted electronically. Notably, the 2006 amendments expanded the definition of "document" under Rule 34 to include ESI, such as Microsoft Word, Excel and PowerPoint files, Adobe PDF files, database records, and CAD/CAM files.[53] The 2006 amendments to the Federal Rules also reaffirmed a party's obligation to adequately preserve relevant documents, including ESI.

Whether a party's efforts to identify, preserve and collect relevant information are sufficient under the Federal Rules is judged against a standard of reasonableness. When dealing with e discovery, the starting point for determining what is reasonable begins with the famous *Zubulake* decisions, authored by Judge Shira Scheindlin of the Southern District of New York. Most recently, in *Pension Committee v. Banc of America Securities, LLC*, Judge Scheindlin reiterated that "the duty to preserve means what it says and that a failure to preserve records – paper or electronic – and to search in the right places for those records, will inevitably result in the spoliation of evidence,"[54] and sanctioned numerous plaintiffs, some with an adverse inference. And yet despite the guidance given to litigants during the past five years or so from "think tanks" such as the Sedona Conference and the ever-expanding body of case law, reasonableness remains relatively undefined and dependent on the facts and circumstances of each case.

What *is* known is that the failure to take reasonably appropriate steps to preserve relevant information and to perform a reasonable search of pertinent repositories could result in sanctions for spoliation of evidence.

And though there is a dearth of case law about what is "reasonable" in terms of identifying, collecting and preserving data in the "cloud," the reasonableness standard undoubtedly applies to efforts in the cloud as well as other locations of ESI.

Rule 26(f) issues

Knowledge of the cloud provider's policies related to the identification, preservation and collection of your data is crucial for purposes of meeting your Rule 26(f) obligations. Rule 26(f) requires that parties meet early in the case to discuss, among other things, "any issues about disclosure or discovery of electronically stored information, including the form or forms in which it should be produced."[55] In today's discovery landscape, it is critical to come to Rule 26 conferences with a full understanding of potential e-discovery issues. If disputes about the reasonableness of preservation and/or collection efforts of ESI arise, the parties should raise them with each other and the court, if necessary, early in the case. Given the fact-specific inquiry with respect to reasonableness of your preservation and collection efforts (and the potential for severe sanctions for failure to adequately comply), it is likewise important to address ESI issues in the cloud, as discussed below, early in the case. These issues include, among others, identification of cloud provider(s) and sub-contractors, data retention and preservation policies for data in the cloud, and terms of access and ability to collect information from the cloud. It is important to raise problems in these areas before you are too far into the litigation and potentially subject to spoliation sanctions.

Notably, Rule 26(b)(2)(B) sets forth specific limitations with respect to ESI: "A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost." The burden is on the party from whom the discovery is sought to show that the ESI is not reasonably accessible. However, blanket assertions that data is inaccessible merely because it resides in a cloud will not pass muster. Understanding the terms of the cloud provider's policies regarding identification, preservation and collection of ESI will help determine the extent to which it is "reasonably accessible," and will provide a basis for negotiating cost shifting, production formats and production timelines.

Getting a handle on what you have

The threshold task in identifying, preserving and collecting relevant information is finding the information. Traditionally, identification of such information involved reviewing the contents of file cabinets and desk drawers for relevant paper documents. And although the process as it relates to

paper discovery is undeniably laborious, there are only so many file cabinets, desk drawers and boxes in which potentially relevant paper documents might be stored. In short, the locations are defined and finite.

The process of identifying relevant ESI, on the other hand, presents a multitude of challenges. Businesses today rely on a variety of electronic solutions for data creation, storage and maintenance. A quick review of the programs installed on an employee's desktop probably reveals an email exchange program such as Microsoft Outlook, document processing software such as Microsoft Word, and a database application such as Oracle for inventory management, customer contact information and accounts receivables. Relevant information might reside in any or all of these locations. And although possibly numerous, these locations are readily known, or ascertainable, by a company's IT personnel and database administrators.

A company's electronic infrastructure typically is created and managed by in-house IT personnel. As such, involving your IT personnel in locating relevant ESI is critical, as these individuals are the masters of data mapping,[56] in that they are responsible for setting up and administering individual user accounts, email accounts, networks, share drives and e-rooms. Thus, they know, or are able to find out, where ESI resides within (and outside of) the company. A party can comply with its discovery obligations by creating a data map, locating and conducting a reasonable search of the data repositories on the data map, and taking appropriate steps to preserve any responsive information.

e-Discovery and the cloud: identification, preservation and collection issues

So what happens when a company decides to outsource data services and storage to a cloud provider? The electronic landscape shifts, leaving a company's data map a little less clear. Unlike documents and traditionally maintained ESI, information in the cloud is not limited to finite areas. A company's data is no longer hosted and managed on networks and servers owned by the company. In fact, a single company's data may be stored on a variety of servers, each on a separate network, and potentially housed in a different country.[57] Identifying and collecting potentially relevant ESI is no longer as easy as having IT walk down the hall to copy someone's "My Documents" folder off of his or her desktop or laptop computer (to use a simple example).

Though cloud computing is a relatively new frontier, for purposes of e-discovery, the goal is to be able to demonstrate to a court that your efforts at all points in the process of identifying, preserving and collecting relevant information were *reasonable*. The following practices will help allow you to argue "reasonableness" at each step, and potentially reduce both costs and burden in doing so. For any of these steps, be prepared to work with a vendor who is knowledgeable about cloud computing issues.

Locating information in the cloud

As with traditionally stored ESI, *know where to find your data*. Before finding yourself in anticipation of litigation, consult with IT personnel to identify a comprehensive list of the company's cloud providers and potential locations of data. In this regard, follow up with the cloud provider to try to determine whether the cloud provider uses any sub-contractors for storing data. Also, be sure to inquire about where the cloud provider physically stores data and whether or not there are any specific issues regarding that data storage that you should be aware of, such as storage format and archiving schedules and capabilities.

Preserving information in the cloud

Cloud-stored data should be addressed in your document retention and destruction policies, as well as in litigation holds. As Judge Scheindlin decreed, the preservation obligation is triggered once a company reasonably anticipates litigation.[58] The first step in preserving data is the issuance of a litigation-hold notice to key custodians as well as to IT; in this new frontier, the hold notice should also be sent to the cloud provider(s). But the mere issuance of a litigation hold is not, in itself, sufficient—companies must take affirmative steps to preserve relevant ESI. Typically, companies must identify the key data custodians and take reasonable steps to preserve their data, be it through the imaging of their hard drives or the targeted copying of their user-created files, ceasing automatic deletion of email, and potentially preserving back-up tapes.

Follow-up steps within the cloud require that companies have a detailed understanding of various cloud provider policies. *First*, what, if anything, will the cloud provider do to implement your legal hold? If the cloud provider will not agree to implement a legal hold (including with respect to any sub-contractors it may use to provide services), it may be necessary to immediately "self-collect" the data before it gets lost or destroyed.[59] *Second*, what are the provider's data-retention and back-up policies? Will it suspend any data-destruction policies with respect to your data? Does the cloud provider outsource its data backup? Try to find out which parties are responsible for conducting, executing

and maintaining the data and backup. *Third*, what is the manner in which the data is maintained? On what kind of cloud is a party's data resident—public, private or hybrid? Is it kept separately from other companies' data? If not, how are different retention policies reconciled (assuming the cloud provider will follow its customers' retention policies)? Is the data "co-mingled" with other data on back-up tapes? If so, how can your data *reasonably* be extracted?

Knowing the answers to these questions will allow legal and IT personnel to make recommendations for data-retention policies and determinations about the need for backing up critical data upon reasonable anticipation of litigation. If the cloud provider will not agree to suspend destruction of relevant information once you find yourself in anticipation of litigation, work with your IT staff or a vendor to make alternate arrangements to preserve data maintained in the cloud.

Accessing and collecting information in the cloud

Collection of relevant electronically stored information can be one of the most costly, technologically demanding and labor intensive parts of the discovery process. Regardless of whether you self-collect or rely on a third-party vendor to perform a collection for you, several issues need to be addressed:

First, know *how* to access and collect your information. Ensure that the cloud provider has access to all data centers used for data storage, so that you are not faced with a situation in which your provider (or you) cannot access your data. Is the company's existing IT infrastructure compatible with the infrastructure of the cloud? If not, costs and the burden of retrieving information can greatly increase. Who can retrieve the information? Does your cloud provider allow for self-collection of custodian files? Are there access restrictions? Who is responsible for the costs to retrieve it—if the company bears the cost, what is it? If self-collection is not an option, you will likely incur the added expense of engaging a vendor to perform your data collections for you. In this regard, you will need to determine if the cloud provider will work with a vendor if necessary.

Second, in what format will the data be collected? As maintained in the ordinary course of business? As with any ESI, if metadata (*i.e.*, creation date, last modified date, etc.) is potentially important to the case, a vendor may be needed in order to preserve the modification, access and creation dates of the collected data. In that regard, costs and the burden of retrieving can greatly increase.

Third, can self-collection be accomplished with minimal upset to your daily computing environment? Or must the collection take place after hours so as not to interfere with server access and bandwidth needs, and if that is the case, what are the costs?

Again, knowing the answers to these questions will help with meeting Rule 26 obligations.

Negotiating with the cloud provider

There are various types of "clouds," including private, public and hybrid clouds. While most public cloud providers offer "take it or leave it" contracts, some cloud providers, depending on the type of provider and/or size of the account, for example, offer more flexibility in negotiating provisions with respect to data retention and preservation, implementation of a legal hold and data collection. At the outset of a relationship with a cloud provider, legal and IT should coordinate to ensure that these bases are covered. If you are able to negotiate, keep in mind the following points (and if you are not able to negotiate, make sure you are aware of the following issues so that you can address them as part of a reasonableness inquiry):

- For purposes of *identification*, know where your ESI will be located at all (or at least most) times. Ask the cloud provider to let you know the location of the servers on which your information will be stored. If you have an issue with certain information being hosted in certain states or countries, make that known to the cloud provider at the outset. Find out who is responsible for maintaining those servers and your data. Determine whether or not any sub-contractors are involved. If so, try to ensure that there is transparency as to who is handling your data, where your data is located, and further, that these sub-contractors will implement the identification, preservation and collection (as well as security and privacy) terms upon which you have agreed with the primary cloud provider. Similarly, the primary cloud provider should have the right to audit any data maintained by sub-contractors to ensure that these policies are properly enforced.
- For purposes of *preservation*, ensure that the cloud provider will implement, or at least adhere to, your data-retention and back-up policies according to your retention schedules. Try to secure agreement that the cloud provider (and any sub-contractor) will take steps to preserve data within a reasonable time frame after

receiving notice. Provide the cloud provider with a copy of your draft litigation-hold letter, and inform the cloud provider of your expectations regarding data preservation once you anticipate litigation. At a minimum, try to get a commitment that the provider will follow your instructions regarding preservation and ceasing deletion of data, including with any third-party sub-contractors. Also, ensure that you can conduct periodic quality control audits to assess the integrity of ESI hosted in the cloud.

- For purposes of *access and collection*, you should also make sure you know how to actually get to your data. Identify any limitations on access to your data once it has migrated into the cloud. Make sure the cloud provider's infrastructure is compatible with your existing IT infrastructure, that metadata will be preserved if necessary or important to your case, and that you will be able to access and collect your data, perhaps on short notice, as it is kept in the ordinary course of business. If your company is subpoenaed, you may need access to your data as it is maintained in the ordinary course of business within a short turn-around time.
- If the cloud provider is subpoenaed for your data, ensure that the cloud provider will notify you immediately upon receipt of the subpoena. You will also want to secure the cloud provider's cooperation in connection with any motion to quash or any protective order necessary to prevent the disclosure of your data. The contract should spell out the cloud provider's obligations in this regard.
- You will also want to ensure that the cloud provider will provide affidavits, declarations, or other testimony as necessary to establish chains of custody and authenticity for purposes of admissibility.
- Finally, try to incorporate provisions that shift associated costs to the cloud provider, especially those costs associated with preserving and collecting data maintained in the cloud.

The failure to address these issues up front could increase your costs in the context of your discovery obligations, and potentially offset any cost savings associated with using the cloud in the first instance. In addition, although untested as of yet, a company that had the opportunity to negotiate these provisions, but either missed the opportunity during the negotiations or otherwise waived these rights, may be subject to sanctions and penalties at a later date.

Call to action

Meeting discovery obligations when data is stored in the cloud need not be daunting. As a preliminary matter, identification, preservation and collection efforts can be more "reasonably" managed, reducing costs and lessening the inevitable burden, by managing data-retention pre-litigation. Reed Smith's e-discovery and technology specialists can provide guidance, create accurate and up-to-date data maps, and draft retention policies that comply with all laws governing retention of particular information, thereby helping to minimize e-discovery costs down the road, including costs associated with retrieving data from the cloud.

If possible, you should negotiate "up front" the issues noted above, which will help minimize the burden and costs associated with e-discovery in the cloud, and also help to establish that you have taken reasonable steps in connection with meeting your discovery obligations. Reed Smith's e-discovery and technology specialists can work with your IT and purchasing departments and assist in negotiating these provisions.

Many providers, however, offer "take it or leave it" contracts. If that is the type of agreement you have already entered into with a cloud provider, it is still critical to know the terms of your contract, to take reasonable steps to identify, preserve and collect relevant data in light of these terms, and, as discussed above, to be able to demonstrate that you took reasonable steps given the terms of the cloud provider's contract. You must also be able to explain the terms of your agreement with the cloud provider to a judge if necessary (for example, to the extent a dispute arises regarding the reasonableness of any of these steps in connection with a Rule 26(f) conference). Again, Reed Smith's litigators and e-discovery authorities have deep experience in this regard, and can assist in investigating and taking the steps necessary to create this record.

Conclusion

In light of the discussion above, one conclusion an attorney advising business enterprises might reach is that cloud computing is far too complex and risky for adoption, especially given the legal risks inherent in electronic discovery and the production of evidence. While some may get away with that for a short time—fear of something new is often a powerful driver—companies may well soon discover that the benefits of cloud computing far outweigh the risks, and perhaps the risks are far more manageable with prudent counsel and some careful management than one might suspect on first impression. The key to

successful cloud computing is to understand the risks, address them as best as one can from the outset of a client/customer/cloud provider relationship, and continue to monitor the cloud, knowing and being fully informed of the risks and the rewards.

References

Wayne C. Matus, Todd L. Nunn and Tanya Forsheit. *Cloud Computing: Emerging E-Discovery Trends – Meeting the New Discovery Challenges in Electronically Stored Information*. Retrieved May 4, 2010, from http://www.straffordpub.com/products/cloud-computing-emerging-e-discovery-trends-2010-05-04. Webinar attended May 4, 2010.

Legal Implications of Cloud Computing – Part One (the Basics and Framing the Issues), http://www.infolawgroup.com/2009/08/tags/security/legal-implications-of-cloud-computing-part-one-the-basics-and-framing-the-issues/ (posted Aug. 18, 2009 by David Navetta).

Legal Implications of Cloud Computing – Part Two (Privacy and the Cloud), http://www.infolawgroup.com/2009/09/articles/breach-notice/legal-implications-of-cloud-computing-part-two-privacy-and-the-cloud/ (posted Sept. 30, 2009 by Tanya Forsheit).

Legal Implications of Cloud Computing – Part Three (Relationships in the Cloud), http://www.infolawgroup.com/2009/10/articles/cloud-computing-1/legal-implications-of-cloud-computing-part-three-relationships-in-the-cloud/ (posted Oct. 21, 2009 by David Navetta).

Legal Implications of Cloud Computing – Part Four (E-Discovery and Digital Evidence), http://www.infolawgroup.com/2009/11/articles/cloud-computing-1/legal-implications-of-cloud-computing-part-four-ediscovery-and-digital-evidence/ (posted Nov. 27, 2009 by Tanya Forsheit).

Trent Livingston and Richard Kershaw, *The Impact of Cloud Computing on Corporate Litigation Preparedness for Clients of Reed Smith*, LECG™ XPRT Forum™, March 2010, at 4.

Michael P. Bennett, *Negotiating Cloud Computing Agreements*, Law Technology News (March 11, 2010), available at http://eddblogonline.blogspot.com/2010/03/negotiating-cloud-computing-agreements.html.

Edward Pisacreta, *A Checklist for Cloud Computing Deals*, Law Technology News (April 9, 2010), available at http://eddblogonline.blogspot.com/2010/04/checklist-for-cloud-computing-deals.html.

Stuart Levi and Kelly Riedel, *Cloud Computing – Understanding the Business and Legal Issues*, printed in Vol. 2, Issue 2 of *Practical Law Journal*, March 2010, at 34.

Special thanks to Allison Jane Walton, Esq., E-Discovery Specialist at Applied Discovery, Inc., for her insights.

— CHAPTER 5 —

Cloud Computing – A German Perspective

Chapter Authors

Thomas Fischl, Counsel – tfischl@reedsmith.com

Katharina A. Weimer, Associate – kweimer@reedsmith.com

Introduction

Traditionally, companies have devoted significant percentages of their overall budget to managing, supporting and scaling their own IT systems and networks. A company's growth and the size of its IT infrastructure typically have had a direct correlation. Until recently, a company's IT infrastructure options were restricted to incrementally scaling up internal capacity or outsourcing to third parties, all or some portion of the IT infrastructure. While the build vs. buy paradigm offers a variety of benefits and challenges, the balance—indeed the benefits and challenges—are in a constant and dynamic state of review and re-evaluation. Especially in an economically challenging environment, companies eagerly search for new solutions to their IT sourcing challenges—solutions that offer reliability, scalability, security, and a difference in their capital and operating expense budgets.

Cloud computing has recently risen to the forefront as potentially one of the most dynamic and most flexible solutions, to solve these companies' IT infrastructure needs with an innovative, cost-effective model. Cloud computing is the term ascribed to the industry shift and transformation from companies either hosting and managing their own applications and data on local servers, or entering into hosting arrangements with third-party providers, to a grid computing model in which users access a shared computing environment typically being provided by large and well-entrenched technology companies.

As we explain below, cloud computing may not necessarily be the silver bullet for German companies or companies doing business in Germany, even if and when it may indeed be an attractive alternative and viable option.

Duties of the Customer

Companies that arrive at the decision to host all or some of their systems within a cloud computing environment will have responsibilities both before the transition and throughout, and these commitments are often paramount to the success of their experience. Principally, customers must identify the nature of the cloud services best suited for their needs (public vs. private cloud hosting), both current and future, and source them from a cloud computing provider that is best able to carry out those services. Great attention to detail is necessary, and the individual departments within a customer's organization must cooperate and communicate with each other to understand both the micro- and macro-issues, and also paint a complete picture of the levels and types of services, hosting and support that the business units require.

Moreover, as a company's needs become more narrowly tailored and specific to certain types of applications, levels of security, support, and the like, the company must either be prepared to negotiate them into the cloud computing agreement or assume them itself and explore means by which the company can work alongside whatever service and support is being offered by the cloud computing provider.

Another fundamental responsibility (and perhaps the foremost such duty) that each cloud computing customer must understand and embrace is the continuous supervision that is required to monitor a company's cloud service. Cloud computing will often afford a customer the ability to change its IT staffing needs, but not eliminate them altogether. Furthermore, depending on the industry and regulatory requirements under which a company may be subject, there may very well be a statutory obligation on the party of the customer to monitor its network, data and suite of technology that has been moved onto some provider's cloud. If the customer cannot adequately supervise the provider itself, it must delegate this obligation to a third party who can.

Lastly, while cloud providers are generally well equipped to provision cloud computing services, a customer must still be certain that it has the requisite bandwidth, capacity, know-how and personnel to host and operate whatever

systems, applications and services remain internally. Customers should also be prepared for change—in terms of protocol, process and security. That which existed previously might be very different from a cloud provider's requirements, and rather than run into a constant state of conflict with the provider, a customer may simply have to change the way it does business in some respects.

Key Concerns of Customers

Cloud computing raises many questions for all parties involved. Customers will generally concern themselves with the following topics:

Contractual Parties

A German customer is likely to prefer a single German provider with whom it enters into a cloud computing services agreement, as the legal implications on many levels will be less onerous and worrisome. A customer will also likely aim to have a single contractual partner that is able to provide a one-stop, turn-key service instead of having to source services from amongst various providers (German or otherwise). While sourcing from various providers might provide a more tailored cloud experience and service, the resources a customer would require to coordinate and monitor its different cloud providers will likely be burdensome and eliminate any cost saving realized through the cloud. Additionally, error-free service is difficult enough to achieve with one provider, but having to coordinate different systems, programs, interfaces, and even operational approaches amongst several providers would likely trigger a multitude of errors, the detection of which could be very challenging.

Support

Support is often neglected in contractual arrangements, but is vital in the daily use of the cloud, particularly at the outset. Customers should seek to have personal support available to them at least during regular business hours, via phone, email and the Internet, and especially in case of emergency. The transitions involved in integrating new IT services, from file transfers to implementation, security, and privacy audits to account creation, often require some level of hands-on support. A customer must ensure and feel comfortable that a provider has the resources to carry out these tasks, and systems and processes are firmly in place to avoid business interruptions.

Right to Use vs. Obligation to Use

The customer should ensure that it is able to use the cloud services at any time and for any amount of time, without the obligation to use and/or pay for them continuously.

Scaling of Services

Even prior to a the onset of contractual negotiations, customers and their service providers must communicate and have some understanding of their needs both in the present and future, and must ensure that a provider will be able to meet those needs if and when they arise. By not having this conversation as early in the process as possible, customers may find themselves having to either add other providers to their hosting stable or move their entire system elsewhere, thus entailing considerable effort. The parties should feel reasonably comfortable that a provider possesses the ability to expand the scope of its services when necessary in return for appropriate consideration. If the provider is unable to commit to offering extended services, the customer may wish to consider other providers.

Sub-Contractors

The cloud provider needs to ascertain whether it can provide all services within its own structure or whether it requires the support or facilities of sub-contractors for certain services. The customer, in turn, should determine for itself whether it is willing to accept a series of secondary service providers, all of whom answer to a single primary provider, or whether it should continue to look for one very large cloud computing provider that either, itself, has a large enough cloud, or one that has a global footprint.

Access to Own Data

The customer must have access to its data at all times, and it is crucial that the data be in a format that other applications can process. The agreement should also plan for the unlikely event of a termination, a provider's refusal to cooperate and/or its insolvency. In all of those potential scenarios, mechanisms should be put into place to ensure continuous availability and access of the customer's data.

Audit Rights

Audit rights are of vital importance for the customer, and the cloud provider should be required to grant the customer extensive audit rights, particularly with regard to data security. While a provider may be somewhat reluctant to extend blanket audit rights or insist upon a narrow scope of those rights, data security carries enough importance that a customer should heavily negotiate these provisions. Just a few of the concerns a customer may have that would be revealed in an audit include, the provider storing the customer's data in cloud locations across the globe, transferring data between various locations without prior

notice to the customer, or using parallel storage of data for a multitude of customers on the same servers (which, in some instances, may even be competitors).

Contractual Constellations

As the foregoing establishes, a customer may be best served if it sources the cloud services from a single provider as opposed to several independent providers. However, such cloud providers only provide the cloud itself and do not transfer the data to the cloud. The customer must therefore negotiate the data transfer in a separate agreement with its carrier. In order to ensure that the cloud provider can fulfill its obligations properly, and to avoid unnecessary complications, the customer should aim to find a carrier that is able to provide the bandwidth necessary for the transfer of data envisaged in the agreement with the cloud provider. The service levels of the two agreements should correspond to each other.

In light of this background, a cloud provider's ability to offer additional carrier services, whether itself or through a sub-contractor, could be a unique selling point.

Type of Contract

German law "recognizes" certain types of obligatory agreements that are individually codified in the German Civil Code. Examples of these include lease agreements, work agreements or contracts of sale. These codified agreements or contracts are not conclusive, though. There can also be mixed or hybrid type-agreements, as well as contracts "sui generis." Depending on the type of contract, the legal consequences, such as warranties, possibilities of termination and even the actual obligations, vary. Yet, even in the case of mixed or hybrid agreements, the consequences will often be determined by identifying the legal character of the main component of the agreement. Although this is not a universally binding rule, it's a relatively reliable guide.

Cloud computing contracts are likely to fall into this category of mixed or hybrid agreements, as they often contain several different services and obligations all under a single *roof*, ranging from the provision of services to the hosting and maintenance of data. There may also be a lease component for the storage space or a professional services element in case customization and development is required to make specific software tailored to meet the customer's needs.

Many of these agreements will also place heavy emphasis on the leasing/licensing of software—the backbone of the cloud. Both parties also need to be aware of the peculiarities of lease agreements under German law, which include an express obligation for a lessor to maintain the leased object in a condition suitable for its purposes. This implies a warranty obligation for the duration of the agreement (*i.e.*, the cloud provider has to remedy defects during that period). However, this obligation does not require or stipulate a certain level of performance, rather only that the cloud and its services are maintained in the state upon which both parties have agreed. Service levels, including response times, downtimes, availability and other parameters, need to be determined in the agreement, typically in schedules to the framework agreement.

Back-to-Back Agreements

Some cloud providers are able to provide their services without having to involve third parties such as sub-contractors. In our experience to date, however, the majority of German cloud service providers are relying on sub-suppliers. These providers will need to agree on so-called *back-to-back agreements*.

The expression "back-to-back agreements" implies that cloud providers, as the party directly responsible to the customer, should pass not only the commercial and technical issues for which they are responsible to the sub-contractors, but also the legal issues, in particular exposure to liability. If it does not do so, the cloud provider may find itself in a situation where it is liable to the customer for certain malfunctions or damages that are, in fact, the sub-contractor's responsibility, and the provider will have no recourse to relay these costs to the sub-contractor.

Experience shows that in practice, back-to-back agreements often are not concluded until the "main" contract between the service provider and the customer has been finalized. At this stage, the sub-contractor is in many cases not willing to accept the risks of the service provider. Thus, the cloud provider should conduct parallel negotiations with both the customer and its sub-contractor(s).

Copyright, Indemnification and Licensing Issues

With regard to copyright issues, the cloud provider should make sure that it is entitled to use the software in the cloud for its intended purposes. This is typically not a problem where the cloud provider owns the intellectual property rights to the software, as the customer will receive a license to such technology, subject to appropriate restrictions on use. From the customer's perspective, it should ensure the cloud provider agreement includes sufficient rights, representations and warranties to use the software in all territories where the customer is likely to do

business.

A greater challenge arises in connection with proprietary software of a third party or open source software. Traditional third-party software licensing policies would restrict a cloud provider from making the software available as part of a service free of the typical restrictions. Therefore, these cloud providers must ensure that they have secured modified rights from the third-party licensors.

Further, as a general rule, cloud providers require indemnities against any claim that is made against them as a result of any information, data or electronic material that a customer places in its cloud that causes it to breach a third-party's IP rights, or violates other rights, be it a third-party's personal rights, or regulatory or criminal requirements and prohibitions. Customers should be prepared to offer these concessions.

Data Protection and Data Security

As cloud computing transcends national borders, one of the major areas of concern arises from compliance with German and European data protection laws. Data security must be a crucial issue in any company's data security analysis.

It can be assumed that cloud computing generally involves the collection and use of personal data. Depending on the exact scope of the services, the parties must assess whether the Telemedia Act (Telemediengesetz, the "TMG") and/or the Federal Data Protection Act (Bundesdatenschutzgesetz, the "DPA") applies. While the DPA is the primary legislation regulating the collection and use of personal data, the TMG governs all electronic information and communication services except pure telecommunication and broadcasting (so-called "Telemedia Services"; *e.g.*, web shops, mobile commerce, newsgroups, music download platforms, video on demand, but not live-streaming of video, web-casting, IPTV or VoIP).

At the core of German data protection laws is the requirement that the party (data controller) that decides the purposes for which any personal data is held or processed, and the manner in which it is held or processed, has sole responsibility for safeguarding the data. This includes ensuring that the data controller retains such data under its close control even when the same data is processed by a third party. Understandably, the requirement distinction does not fit easily into the cloud model.

According to German law, data processing by a third party on behalf of the data controller is explicitly regulated in the DPA (section 11, DPA). It requires a written agreement between the data controller and the data processor that describes the agreed data processing services in detail, and must contain certain specifics, which are *inter alia*:

- The technical and organizational data security measures employed by the third-party data processor; this includes by means of law that the customer/data controller is not simply obligated to question and investigate these measures, but is also to effectively check whether the measures are in place and work properly
- Information on the correction, deletion and blocking of data
- Potential sub-processing, if applicable, and allowing for respective arrangements with sub-processors
- Control rights of the data controller and corresponding co-operation duties of the data processor
- Return of data and deletion of data at the data processor's premises

However, inherent in using a cloud provider as a data processor is the loss of control over the processing of data when compared with using a hosted data centre. This causes some conflict with the restriction in German and European legislation on the international transfer of personal data. Data transfers outside Germany must pass two tests:

- Any data transfer constitutes the processing of personal data and requires the consent of the individual whose data is being transferred unless statutory permission exists
- Data transfers outside the EEA are prohibited if the data subject has a legitimate interest in the prevention of the data transfer (sections 4b(1) and (2), DPA). Such legitimate interest is statutorily assumed if and where the recipient does not provide for a level of protection adequate to the protection in the EEA.

In particular, the European Commission has made findings that the United States does not offer an adequate level of protection. Data transfer to a recipient in the United States is therefore permitted only if additional requirements (*e.g.*, compliance with Safe Harbor principles or conclusion of a model contract) are met.

This issue is not merely academic, as these restrictions directly conflict with one of the central efficiencies of operating in the cloud, namely, that the provider can seamlessly move its customers' data between and among

its global network of server banks.

German data protection laws also impose a duty on cloud customers to ensure their data processors hold personal data securely. According to the law, this includes the obligation that a customer, as data controller, visits the processor's (*i.e.*, cloud provider's) premises to ascertain whether the required security measures are in place. While it is highly impractical for the German customer (or any customer for that matter) to visit all server locations of the cloud provider for verification of the security measures, this is in theory the requirement imposed by the law. So far, there has been little guidance or comment from the German national data protection authorities on how cloud computing fits within the existing data protection laws and what, if any, particular security measures should be taken.

Cloud providers (as any click-wrap agreement licensor) typically place broad exclusions of liability in their terms of service and do not guarantee compliance with national data protection laws. Companies with strong personal data ties or that regularly collect, aggregate and process (or have processed) other highly sensitive forms of data, in particular, should carefully consider if and how best to transition their business functions into the cloud.

Confidentiality

Data confidentiality is of vital importance to every company across all industries, especially when data sits in the hands of third-party sub-contractors of any kind. Not only must the cloud provider, itself, maintain confidentiality of its customers' data, but it must also extend this obligation to each of its sub-contractors. Providers must also ensure that sufficient transparency exists to allow a customer to review the measures implemented to maintain such confidentiality. The latter point will be difficult to accomplish, though, as the cloud provider will not always agree to provide the necessary insight and transparency to its customers.

Legal Enforcement

An important point to be taken into consideration is the difficulty a customer may face in enforcing its potential claims against a cloud provider. It is commonplace in the IT business to discontinue certain services, amend/modify software or hardware, or relocate customers to other services that are more economically efficient for the service provider. All of these actions could possibly result in disastrous situations for the customer who has relied on the availability of the services and the outplaced data. In theory, the agreement should provide for a multitude of legal remedies to cover these situations. However, even if German law is applicable and the German customer is able to push for a German venue, the legal remedies are usually not sufficient to ensure immediate assistance for a customer. Even the swiftest form of a legal remedy, a preliminary injunction, will generally take a few days to obtain. That can be too long a period when a customer needs to access to data and/or when a customer's business has been severely impeded. A proceeding on the merits can only serve as a retrospective appraisal of the situation and an assessment of warranty or damage claims.

If the cloud provider is not in Germany, and applicable law and venue are also outside Germany, the possibilities of legal enforcement for a German customer will diminish even further.

Summary

In Germany, cloud computing is still in its infancy. Many of the major providers are currently trying to identify their principal markets, thus reflected in many of the loose service descriptions and relatively generic terms that have been batted around as of late. However, regardless of a number of open technical and legal issues, consulting firms recommend dealing with cloud computing, and at least recommend experimenting with cloud computing in order not to miss out on a very promising technical trend.

— CHAPTER 6 —

Cloud Coverage

Chapter Authors

Richard P. Lewis, Partner – rlewis@reedsmith.com

Carolyn H. Rosenberg, Partner – crosenberg@reedsmith.com

Introduction

Where clouds form, rain follows. Insurance should be there to protect you. This article outlines steps to consider so that coverage holds when the rain hits.

Cloud Computing may create new risks and exposures, financially as well as reputationally. Traditional and more recent insurance coverage may come into play. On the traditional insurance front, property, and specifically business interruption coverage, may be a natural place to look. These policies are designed to cover first-party exposures—loss to business. Other coverage to consider for claims made by third parties against a company—by stockholders, consumers, the government or other entities—include commercial general liability ("CGL"), professional liability, director and officer liability, employment practices, and fiduciary liability policies. More recently, data privacy and security policies (sometimes called "cyber" policies) should be considered as well.

First-Party Coverage Issues

Cloud Computing Purchasers

The primary first-party exposure is to Cloud Computing consumers, where some event impacts their data or ability to access that data, causing them to lose income. Is this lost Business Income covered under standard first-party policies providing Business Income, Contingent Business Income or Service Interruption coverage?

Business Income coverage is designed to cover a policyholder for loss of profits and unavoidable continuing expenses—"Business Income"—during the period business is affected by damage to property through which the policyholder conducts operations. *Contingent Business Income* coverage is designed to cover a policyholder for lost Business Income when damage to property through which a third party conducts operations prevents that third party from providing services to the policyholder. *Service Interruption* coverage is designed to cover a policyholder for lost Business Income when certain enumerated services provided to the policyholder are interrupted, typically by damage to off-site transmission or generation equipment. Because it is unclear whether any of these coverages, as typically drafted, would cover a Cloud Computing consumer for lost Business Income from damage to, or inability to access, their data, new coverages will need to be drafted.

As to Business Income coverage, note first that such coverage is typically restricted to damage to property at (or within 1000 feet of) the premises, and it seems likely that any damage to property causing a Cloud Computing interruption would not be located at the premises of the policyholder: indeed, one of the prime advantages of Cloud Computing is that the "property" is off-site. It is hard to predict where damage to data would be deemed to have taken place. Indeed, courts may not consider data to be property, susceptible to damage, at all.[60] Relatedly, courts may find that data that simply cannot be accessed has not been damaged. Most courts, however, find that property that cannot be used for its intended purpose has been damaged.[61]

Because a claim based on the inability to access data as a result of problems of a Cloud Computing provider would likely involve data or equipment off-site, it would appear to fit more naturally as a Contingent Business Income claim. Again, however, the policyholder would have to prove that damage to property caused the interruption.

A claim under most Service Interruption provisions would fail because they are limited to the most common services provided a generation ago: electric, steam and telephone services. Further, most such provisions require property damage from a covered cause of loss.

As to all of these coverages, computer or data-related losses are frequently (1) excluded; (2) subject to strange limitations;[62] or (3) subject to extremely small sublimits.

Relatedly, such coverages are frequently subject to dollar as well as time (*e.g.*, 24 or 72 hours) deductibles. Redundancies in the operations of Cloud Computing providers will likely limit the duration of the problem, meaning that the deductibles swallow the potential coverage. Nonetheless, any problem may completely shut down a Cloud Computing consumer, causing them to lose a great deal of income. It may also cause the policyholder's customers to turn elsewhere for a time after the interruption, perhaps permanently.

What likely is needed is for policyholders with large Cloud Computing exposure to purchase specialty insurance covering them for loss attributable to loss of, or inability to access, their data, above a clearly identified (and ideally small) deductible. Such coverage must include extensions for the period of time in which losses continue after the interruption because of loss of customer goodwill.

Fidelity bond coverage (which is required by regulation in some industries) is also important to assess. Theft, extortion, and cyber-related loss may be covered. Fidelity bond policies have strict requirements for reporting a loss and filing proofs of loss. Failure to adhere to the deadlines can preclude coverage.

Third-Party Coverage Issues

Third-party exposures may include claims related to websites, data control, errors in privacy protection, defamation, theft, consumer class actions, securities claims and government investigations. Claims may be brought domestically and internationally. The availability of third-party coverage will depend on the type of claim and other terms and conditions in the policies. A brief explanation of potential policies includes:

Director and Officer Liability Coverage—One can envision a potential claim against directors and officers of a company for failing to supervise a Cloud Computing initiative or for being "asleep at the switch," and thereby breaching their fiduciary duties. One can also imagine the Securities and Exchange Commission investigating, or shareholders suing, a company for insider trading, restatements, or financial misrepresentations in disclosures in connection with Cloud Computing investments, insider deals, or other exposures that cause a stock drop or serious financial problems. A D&O policy typically covers directors and officers for claims made against them when the company cannot indemnify them. The policy also reimburses a company for amounts it indemnifies the directors and officers and, if entity coverage is purchased, the policy is designed to cover securities claims made against the company. Coverage will depend on the specific terms, conditions, and exclusions in the policy. Companies should be vigilant in reviewing the coverage to narrow exclusions and seek coverage enhancements.

Professional Liability/Errors and Omission Coverage—Professional liability coverage is designed to cover claims made against the company and its employees for alleged acts or omissions in the context of doing their jobs. This coverage should also be examined and negotiated to avoid specific exclusions that could impair coverage.

Fiduciary and Employment Practices Liability Coverage—Employee benefit plans and stock option claims involving potential fiduciary and trustee liability may be covered under a fiduciary policy. And if employment practices claims such as discrimination, sexual harassment or hostile workplace environment are made, such coverage may be reviewed.

Comprehensive General Liability Coverage—A CGL policy typically provides coverage for bodily injury and property damage, as well as for advertising and personal injury. The definition of "property damage" may exclude electronic data in some policies, and should be addressed as it may be possible to negotiate an endorsement to provide such coverage. "Personal injury" claims may include publication or utterances that violate an individual's right of privacy or are defamatory or disparaging. Exclusions, however, may limit the breadth of coverage.

Data Privacy and Security Coverage

Data privacy and security policies may provide both first-party and third-party coverage. For example, some technology, media, data privacy breach and professional liability policies provide coverage for first-party loss, including internal hacker attacks or business interruption, or expenses to maintain or resurrect data. Coverage for third-party loss may include reimbursement of defense costs and indemnification for judgments and settlements. The claims may include allegations of violations of privacy rights, and personal information, duties to secure confidential personal information under state and federal laws and regulations, breaches by employees or others, infringement of intellectual property rights, unfair competition, defamation and consumer protection, and deceptive trade practices statutes. The coverage may also include regulatory actions, lawsuits, and demands. Coverage may additionally apply to "breachless" claims, where a potential problem or disclosure can be fixed before it becomes a claim. The policies are relatively new,

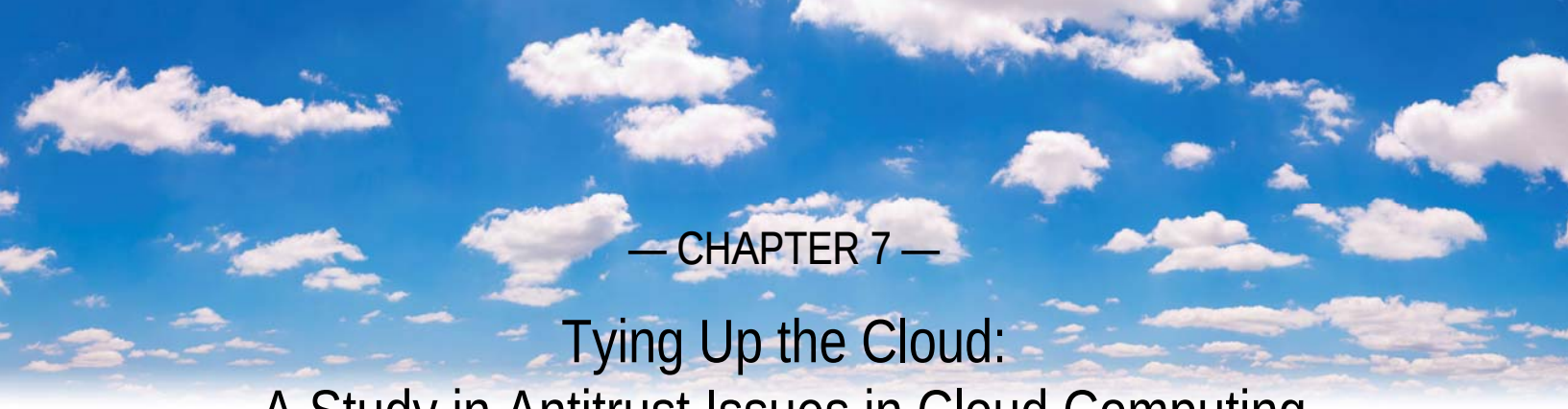
however, much as employment practices liability policies were 10 years ago. The data privacy and security policies are negotiable and should be analyzed with a coverage lens to reduce uncertainty and broaden coverage for targeted exposures.

Maximizing the Potential for Insurance Recovery

Although no policy is foolproof, the following steps can be taken to keep coverage umbrellas functioning. Working with knowledgeable coverage counsel:

- Inventory all potential policies now. Review any indemnification agreements with vendors or third parties who may owe contractual obligations to the company.
- Analyze the terms and conditions on a "what if" basis, so that companies can determine potential exclusions or terms and conditions that may impact recovery.
- Compare policy forms on the market and negotiate a "wish list" of potential items to clarify and enhance coverage.
- On an annual basis, take advantage of advances in the insurance market and be aware of coverage decisions in the courts.
- If a breach, loss, or claim occurs, know whether, when, how and why to report a claim or potential claim.
- Obtain consent to defense arrangements if the policy requires.
- Keep the insurers informed of claim developments and respond to reasonable requests for information and cooperation.
- Seek consent to settlements and payment of loss or judgments on a timely and informed basis.
- Know the dispute resolution and choice of law provisions in the policies, including the excess insurers.

With knowledge, vigilance, and persistence, cloud coverage—protection when it rains—is possible.



— CHAPTER 7 —

Tying Up the Cloud: A Study in Antitrust Issues in Cloud Computing

Chapter Author

Jeremy D. Feinstein, Partner – jfeinstein@reedsmith.com

The cloud computing era represents a significant shift in relationships in the information technology field. This shift will raise many antitrust questions, among other legal issues. Many antitrust questions will not become apparent until cloud computing business models become better established, but some issues are readily apparent even at the threshold. For instance:

- After a customer selects a particular cloud provider, can the customer be "locked in" to particular products and services within that cloud?
- When will a cloud provider be permitted to exclude other service providers or software providers from participating in a cloud?

This article provides some preliminary thoughts on these questions and considerations that should be taken into account by organizations providing and considering purchasing cloud computing services. Although definitive answers to these questions always require a specific factual context, the discussion below identifies some fundamental antitrust principles that apply and may help prospective cloud purchasers understand their rights and avoid potential traps by negotiating prudent contract terms when entering into a cloud computing arrangement. The key for prospective cloud purchasers (*i.e.*, users of cloud computing services) is to obtain complete and accurate disclosures of a cloud provider's after-market policies *prior* to the initial decision to enter the cloud. After the initial purchase of cloud computing services, customers may find that their bargaining power is dramatically reduced by switching, compatibility, interoperability or even early termination costs.

A Starting Point: Power in the Cloud Services Market

Antitrust questions that are raised, and the range of possible answers that should be considered, will depend in significant part on (a) the definition of the "relevant market" in which a given cloud provider competes and (b) the determination whether the cloud provider has the ability to influence prices or output in that market as a whole—an ability referred to as "market power." A relevant market encompasses all products that prospective purchasers in a particular geographic area would consider reasonable substitutes for each other. The relevant market includes not just existing substitutes, but also those that might enter the market within a relatively short time in response to a sustained rise in prices. Antitrust law places many more limitations on the activities of companies deemed to have power within a relevant market than on the activities of companies that lack such power.[63]

Application of these basic antitrust concepts suggests that, at least at this very early stage in the development of cloud computing, it would be very challenging to prove that a cloud provider had "market power" in a putative market for the sale of cloud computing services. First, the market is arguably worldwide: the very idea of portable cloud services implies that a cloud provider in Canada could compete with a cloud provider in Australia for customers in the United States. Second, at least for now, the relevant market arguably cannot be limited to the provision of "cloud computing services" alone because for most companies and most business purposes "old fashioned" hardware and software systems and third party hosting arrangements, though lacking many of the benefits afforded by cloud computing, still remain reasonable substitutes for clouds. Third, the number of potential new entrants into the hypothetical market for cloud computing services is still uncertain, and could prove to be very large.[64] Cumulatively, these factors suggest that until cloud computing develops a

bit further, the provision of cloud services will be a market with many actual and potential competitors, reducing the chances of particular providers attaining real market power.

One possible exception to this could be hypothetical future clouds that are explicitly focused on delivering products or services already powerful in their fields, such as clouds for Apple iTunes, Microsoft Office, or the Google search engine. These cloud scenarios may not remain hypothetical for long.[65] Enterprising plaintiffs might assert that the cloud providers have market power in putative markets for the provision of these specific cloud services, just as they might assert such power independent of the cloud context. But even for distinctive examples like these, it is not clear that the cloud context will change the power analysis much from the pre-cloud era, and in fact the cloud context may be dilutive: a new spreadsheet program seeking to compete with Excel, for example, might have an easier time doing so "in the clouds" than it would have in the past, where placement on "traditional" desktop and laptop hardware was a prerequisite for entry.

After-Market Analysis: Power Within A Cloud

A more likely scenario in which cloud providers may face credible near-term allegations of market power is in "after-markets" for products and services within their own clouds. The antitrust concept at work here is that there could be separate markets for the "provision of cloud computing capabilities" and the "provision of services or software products within a cloud." A cloud computing vendor might face substantial competition from other clouds in a "primary market" where the customer chooses among various cloud providers, while at the same time facing little or no competition in "after-markets" for selling particular services to customers already in its cloud.

The possibility of cloud service providers exerting power within their clouds is certainly not limited to services involving already well-established brand names. Cloud computing customers may come to value or require any number of after-market services in their clouds, and cloud providers may attempt to dictate or limit customer choices with respect to such services. For instance, a cloud provider might insist that any cloud customer utilizing its data storage services also purchase and utilize the provider's own proprietary virus detection software. Would such a limitation injure the cloud customers, or other potential vendors of virus detection software, in a way that the antitrust laws might redress?

The well-known Supreme Court case of *Eastman Kodak Co. v. Image Technical Services*, 504 U.S. 451 (1992), is the most authoritative example of after-market antitrust analysis, and the principles it articulated remain highly instructive. *Eastman Kodak* is worth considering in detail because it provides a virtual checklist of potential after-market risks that companies purchasing cloud computing services should be mindful of when they choose a vendor.

When Is An After-Market A Relevant Market?

Lock-ins, switching costs, and information barriers.

In *Eastman Kodak,* the plaintiffs were a group of independent servicers (ISOs) of sophisticated copiers made by Kodak. Kodak faced strong competition and lacked market power in the primary market for the sale of copiers. At the same time, Kodak faced only no competition in the after-market for the sale of replacement parts for Kodak copiers (which parts were only available from Kodak or its licensees) and only modest competition from the ISOs for the sale of repair services. When Kodak attempted to further increase its share of the services after-market by selling replacement parts only to customers who also purchased repair services from Kodak, the ISOs sued Kodak under monopolization and tying theories.

The Supreme Court held that the ISOs' proposed relevant after-market for the servicing of Kodak copiers was sufficient to survive summary judgment. The Court emphasized that the determination of the relevant market must be made from the perspective of a consumer (here, the purchasers of Kodak copiers), and should include only those products or services that consumers view as interchangeable.

Kodak argued that there was no true distinction between the primary market for copiers and the alleged after-markets for parts and services. Kodak's theory was that consumers could engage in "lifecycle pricing" analysis, and thus the costs of its parts and services policies would inform the consumer's primary purchase decision of what copier to buy. Consequently, Kodak contended that its lack of power in the primary product market should end the issue as a matter of law.

The Supreme Court did not find this persuasive. It concluded instead that Kodak's theory, "although perhaps intuitively appealing, may not accurately explain the behavior of the primary and derivative markets for complex durable goods" because of information barriers and switching costs. The Court observed that the information needed to engage in lifecycle pricing of Kodak copiers was difficult or impossible to acquire at the time of purchase, and in any event was subject to change during the lifespan

of the copier. Thus, the court viewed the initial purchase decision as separate from subsequent decisions to purchase parts or servicing.

Once a customer had made the substantial capital investment in purchasing a Kodak copier, the cost of switching to another copier would be quite high. Thus, Kodak customers were effectively "locked-in" to the parts and servicing prices (and price increases) imposed by Kodak. The Court concluded that "the relevant [service] market from the Kodak equipment owner's perspective is composed only of those companies that service Kodak machines," and that the ISOs were therefore entitled to a trial on the question of whether Kodak abused its power in that market.

Lessons of Eastman Kodak

Eastman Kodak teaches several valuable lessons for prospective purchasers of cloud services who wish to protect their interests (and to do so with less cost than a protracted antitrust suit). First, the switching costs for corporate customers who purchase cloud service are likely to be substantial, and every prospective purchaser should carefully evaluate whether these costs will be high enough to effectively create a "lock-in" with their cloud provider. For example, customers should consider:

- Whether the cloud offers specialized software or services that, once adopted by the customer, would be difficult to obtain from another source
- How large an investment of time and money will be required to train employees to use the cloud's user interface and software
- How quickly and at what cost could data stored in the cloud be retrieved and placed in another cloud or on the customer's own storage systems
- What data security concerns would be implicated and what notifications might be required if the company later decided to move its data to a different cloud

Second, if switching costs will be high enough to create a lock-in effect once a particular cloud is selected, prospective purchasers need to obtain as much information as they can *before* they purchase cloud services about how the cloud service provider will handle after-market services. Prospective purchasers should press a cloud service provider, at a minimum, to:

- Identify all software/services that are or might be included in the price of cloud services
- Explain its policies regarding customers' right to disaggregate services that it does not want
- Identify any software/services that are mandatory
- Explain its policies regarding customers' rights to add or substitute the software/services of providers of their own choosing, including providers who may provide software or service competing directly with software/services of the cloud provider
- Explain its policies regarding future price changes (and perhaps whether a long-term price agreement is available, if that is otherwise in the business interest of the customer)

A customer that takes these steps may reduce its chances of being taken advantage of in after-markets for cloud services.

Addressing Misconduct In After-Markets

What if the prophylactic steps described above fail, and a cloud provider adopts policies in after-markets that its existing customers dislike or that exclude competitors? Litigation based on *Eastman Kodak*-type theories would be an option for customers, as well as for potentially competitive service providers in cloud services after-markets who believe, like the ISOs in *Eastman Kodak*, that they are being harmed. In such a setting, a plaintiff would need to claim that the cloud provider's conduct unreasonably impaired competition in a relevant market in some fashion, not just that it injured the plaintiff in particular.

There are many antitrust theories that an after-market plaintiff might employ, of course, but two of the most likely would be tying claims and exclusive dealing claims. A full discussion of how these theories might apply to cloud computing fact patterns would be premature, but set forth below are a few preliminary thoughts on each.

Tying in after-markets

To bring a tying claim, a plaintiff must show that there are two separate products, that the defendant has "tied" them by conditioning the sale of one on the purchase of the other, and that the defendant has market power in the tying product. *See generally Jefferson Parish Hospital Dist. No. 2 v. Hyde*, 466 U.S. 2 (1984). Tying claims are a natural fit for after-markets, where the seller of the primary product often has a large share of after-market products and services, too. In the *Eastman Kodak* case, Kodak allegedly tied the sale of replacement parts to the concurrent purchase of Kodak's repair services, which

allegedly had the effect of preventing customers from dealing with the plaintiff ISOs.

As already noted, a similar scenario could arise in the cloud context if a cloud provider insisted that it would only sell its data storage services to those of its cloud customers who also purchase the provider's own proprietary virus detection software. A cloud provider would have a much better chance of defending such a policy if it were disclosed to customers prior to their entry into the cloud—with such facts, a cloud provider might be able to convince a court that the virus detection software was not "tied" to anything but was simply part of the original package of services that the customer knowingly chose to purchase. If this policy were adopted after customers were already "locked-in" to the cloud, however, the analysis might proceed in a manner similar to *Eastman Kodak*. That is, if the cloud provider were deemed to have market power in the after-market for the sale of data storage service within its own cloud, conditioning the sale of that service on the purchase of other products or services might expose the provider to an antitrust trial in which the anticompetitive injuries (if any) caused by this policy would be evaluated.[66]

Exclusive dealing in after-markets

Exclusive deals between cloud providers and particular product or service vendors are also a foreseeable source of conflict. Suppose our hypothetical were altered slightly, and instead of tying distinct products together, a cloud provider announced to existing locked-in customers that it had reached an agreement with another firm (say, Symantec) to be the exclusive virus detection software vendor for the cloud. Cloud customers need not purchase Symantec's software at all, but if they want to deploy virus detection software in the cloud, it must be Symantec's. Would cloud customers or competing virus detection software vendors have an antitrust claim based on this new policy?

Exclusive dealing agreements are frequently lawful, but they can violate antitrust laws if they foreclose competitors' access to a substantial share—some courts have suggested 40 percent is in the right ballpark—of the relevant market for their products. This suggests that Symantec's competitors would be unlikely to have a viable claim based on the facts above. No single cloud, at least in the near term, could come close to containing such a large share of the market for the sale of virus detection software.

As to the cloud customers, a threshold question, again, is whether the exclusivity was pre-announced. If IBM offers cloud services and announces from the outset that only IBM software products will be permitted in the cloud, it would be difficult to understand a subsequent claim by a customer that they were harmed by this exclusivity policy. A customer that wants to use Microsoft software should pick a different cloud. If the cloud vendor had reserved a contractual right to control software within the cloud, similar logic might apply. But if cloud customers are already "locked in" and are taken by surprise by an exclusive deal, the analysis might be different. Much like the copier purchasers in *Eastman Kodak*, for a locked-in cloud customer, competition in the relevant after-markets for cloud services consists of the products and services that the cloud provider allows to operate in the cloud. If the cloud provider reached an agreement to exclude competition in those markets, the locked-in customers might have a plausible claim for antitrust injuries (higher prices, reduced quality) resulting from the deal.

Conclusion

Prospective cloud services purchasers need to protect themselves by seeking complete and accurate disclosures of a cloud provider's after-market policies *prior* to the initial decision to enter the cloud—or to contract with a particular provider. Ideally, purchasers who anticipate a lock-in effect, similar to long term outsourcing contracts, should negotiate for terms that limit the ability of the cloud provider to change the rules of the cloud service offerings and pricing in the middle of the contract term. After the initial purchase of cloud computing services, customers may find that their bargaining power is dramatically reduced by the switching costs they may need to incur to both get out of the existing relationship and migrating to a new one—whether in whole or in part. Although many aspects of the cloud computing industry and its players are still in their infancy in terms of technology and economic models, the well-established principles of antitrust law that are increasingly being enforced by governments around the world still very much apply and will likely have a decisive role in how the industry ultimately unfolds both in the short and long term.

— CHAPTER 8 —

Look, Up in the Cloud… It's a Bird, It's a Plane, It's a Bank

Chapter Authors

Joseph I. Rosenbaum, Partner – jrosenbaum@reedsmith.com

Leonard A. Bernstein, Partner – lbernstein@reedsmith.com

Anthony Traymore[67]

Introduction

The financial services industry, being one of the largest global consumers of technology, often serves as a driver of change as new banking and financial products and services are introduced into the information, transaction processing, storage and communications pipeline. Cloud computing as both a product and service of sorts will likely be no exception. The value propositions presented by utilization of cloud computing environments, such as cost containment, immediacy, availability, scalability, efficiency and resiliency, will simply be too attractive for chief operating and information technology officers to ignore. However, as highly regulated businesses, financial services firms will be forced to develop sound policy and governance practices to manage the risks that come with utilization of a third-party IT platform.

The Cloud Computing Primer

There are essentially four models of cloud computing environments available to financial services firms—private, community, public and hybrid.[68] The defining characteristic of a private cloud is that it is operated solely for one organization.[69] A community cloud is often shared by several organizations and supports a community with shared requirements.[70] A public cloud is made available to the general public or a large industry group.[71] A hybrid is some combination of two or more of the three other cloud environments—private, community and public.[72] Private clouds, because they are developed and used solely for the benefit of one organization, extend the most security of the cloud environments. As the sole user of a private cloud, an organization can often set the parameters for information collection, storage, transfer and access to suit its own policies and procedures. Also, the information stored on a private cloud will only be that of the single organization. Community clouds, to the extent the organizations utilizing the community cloud are able to agree, may offer similar data-protection parameters to that of a private cloud. However, a community cloud contains the information of all participating organizations—which means that a firm's information will be stored with that of other organizations, potentially even competitors' at times, if the community cloud is set up to handle the requirements of a specific industry. Public clouds generally offer less flexibility and robustness with respect to customization of information security processes and procedures, but understandably offer greater affordability. They are also more typically limited to the standard options offered by the third-party service provider.

Applicable Legislation and Federal Agencies

When considering cloud computing, the litany of primary legal risks that businesses in the financial services industry, along with their finance, business development and IT professionals and, of course, their lawyers, focus on, cross the spectrum from integrity and reliability to security, identity and privacy (*i.e.*, the handling of non-public personal information ("NPPI")). In the United States, financial services firms are subject to extensive laws, regulations and guidance relating to information security. The Gramm-Leach-Bliley Act of 1999[73] (GLBA) requires that financial institutions safeguard the security and confidentiality of customer information and places certain prohibitions on sharing NPPI with non-affiliated third parties. Moreover, various state privacy laws, such as the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth,[74] also

apply to the extent they impose more stringent security standards than GLBA. To the extent an institution—in some cases these same institutions—conducts broker-dealer activities; underwrites or offers insurance; engages in corporate and consumer banking; lends money; engages in the transmission of money; provides financial advisory, investment or custodial services; issues credit, charge, debit, stored value or gift cards—these and other laws, regulations and requirements apply. Businesses engaged in providing financial services in the United States are subject to these and an increasingly complex web of regulations and guidelines issued by numerous governmental and regulatory bodies, both individually and collectively,[75] such as the Federal Reserve Board, OTS, OCC, FTC, SEC, FFIEC,[76] FDIC and even self-regulatory initiatives developed and implemented by the Payment Card Industry (PCI).[77]

The challenge of compliance and corresponding risk necessarily becomes greater when a firm moves certain operations and functions to third-party cloud computing service providers. Each of the aforementioned statutes and regulatory bodies, as well as the numerous other regulations and guidance documents—several of which are referenced in this document—make it clear that an organization must conduct extensive due diligence on its IT service providers and use at least reasonable efforts to manage and monitor its third-party services providers' compliance with applicable guidelines and regulations. As far as the regulators are concerned, it will ultimately be the financial services firm's responsibility to handle NPPI of its clients and customers in accordance with applicable guidelines and regulations, regardless of whether such information resides on an in-house system or a third-party service provider system. As we said above, we don't know of any cloud-computing exceptions or carve-outs that would conveniently *manage* the many laws and regulations that govern financial services companies.

The principle of "follow the money" has become not only more facile in our age of digital processing and technology, but also increasingly complex. Both Congress and the online gambling industry discovered this back in 2006 when lawmakers finally realized, after years of failed efforts to stymie this explosive business, that the key to encumbering its growth was to stop the processing of financial transactions. The solution—tack an Unlawful Internet Gambling Enforcement Act onto the Security and Accountability For Every Port Act of 2006,[78] which President Bush signed into law October 13, 2006.

Of potentially greater long-term consequence, the financial crisis, coupled with the perceived failure of the current regulatory scheme, helped garner support for the creation of the Consumer Financial Protection Bureau ("CFPB"). Created as part of the Dodd-Frank Act passed by Congress in 2010, the CFPB, housed within the Treasury Department, may well prove to be the most powerful federal agency in the United States. The CFPB has a single mission—to protect consumers. The scope of the CFPB mandate includes the development of consumer protection rules currently the domain of seven different federal agencies. With little oversight, a very large budget, and almost complete independence, the CFPB is likely to have a major impact on the financial services industry—from the manner in which financial services are advertised and marketed, to the disclosures and consumer protection mandates; from the nature of financial services and product offerings to compliance and enforcement measures. That said, it is also important to note that the CFPB doesn't actually replace any of the other agencies—it is intended to be incremental or supplemental to them, adding potentially another layer of regulation, compliance and confusing turf wars to an already complex financial services regulatory landscape.

The Landscape – Reconciling Regulations, Business Requirements and the Realities of the Cloud

Computing Globally

What, then, are the implications for cloud computing? Cloudy, to say the least. With cloud computing platforms, financial institutions may have the capability not only to outsource their technology operations and resources to the cloud, but also to significantly enhance their ability to reach consumers and offer financial products and services anywhere, anytime, with significantly pared down physical infrastructure. Web-based and mobile banking are already rapidly increasing in both availability and consumer adoption. The issue becomes of paramount importance as there is no exception or special dispensation for financial services companies that wish to adopt and integrate cloud computing into their infrastructure. Security, coupled with interoperability, will be as heightened a concern within the cloud as in any other environment, and very possibly more concerning.

Consider the following example: a financial institution wants to outsource its technology and operations to an outsourcing provider in India. In evaluating the transaction, the financial institution needs to evaluate not merely the capabilities of the outsourcing provider to ensure integrity, security, transmission capability and reliability, but both the ability of the provider to ensure compliance with the

banking or financial regulations that apply, and the question of whether the laws and regulations, the judicial system, and law enforcement mechanisms from the jurisdiction in which the outsourced services will be provided, are adequate to ensure that if the contract is solid, the ability to actually enforce it will be as well.

But what if the jurisdiction(s) is a continually floating cloud. As configured today, it will be difficult, if not impossible, to determine or regulate features, functions, services, applications, databases and the like, in a cloud computing environment. Will regulators need to insert a compliance regulator in every cloud-computing company? Will requirements and reporting be so complex and multi-jurisdictional that the perceived benefits of cloud computing will quickly be eaten up by difficult and overwhelming regulatory requirements, perhaps differing ones for differing jurisdictions? Do we need some international convention that countries and states will ratify to normalize cloud computing on a global (or quasi-global) basis? Will governments require cloud computing providers to agree to submit to jurisdiction before a regulator will allow a financial institution to use that provider's services? Will interoperability and cross-service platform agreements need to deal with these issues when one cloud computing provider interfaces with another?

Perhaps we can borrower a paradigm from the telephony universe where point-to-point communications often pass through multiple jurisdictions, carried by multiple carriers, transparent to both the initiator and recipient of the phone call. We rely on the privacy of these communications, in part because of technology, but also based on the fact that most voice telecommunications services are both regulated and protected around the world – most, but not all. Thus, if your telephone call was to be routed through a country that did not have such protections or had different protections – wiretaps, illegal in this country, might not be illegal and could even be routine practice for a foreign intelligence service, a private telecommunications company, or three teenagers with a homemade scanning device! This, in an industry that has been heavily regulated for almost a century. In stark contrast, cloud computing is not a regulated industry or activity. Which brings us nicely to consideration, briefly, of international issues applicable to cloud computing in the financial services industry.

As noted above, financial services firms with operations outside the United States must also be concerned with the foreign laws and regulations governing their operations in every jurisdiction in which they do business - in some cases, not merely different, but inconsistent laws and regulations. For example, the restrictions on firms with operations in Europe with respect to data transfer/sharing and security under the various country-level implementations of the EU Data Protection Directive, are more stringent than those under U.S. law. Suffice it to say, compliance with all applicable information security regulations and guidance, whether federal, state or abroad, is difficult for a financial services firm even in a self-contained IT environment; and yet a firm's failure to properly manage this landscape can be devastating.

Something Old, Something New – How Are Dated Rules and Regulations Applied to Cloud Computing

Returning the focus back to the United States, issues that financial services firms will be forced to grapple with are outdated and less-than-helpful regulations and laws. By way of example, the Federal Financial Institutions Examination Counsel ("FFIEC") over the past decade promulgated a series of guidance statements and policies for financial services companies on IT risk management for outsourced technology services, the latest of which was seemingly released back in 2004 (before the term cloud computing was even a glimmer in anyone's lexicon). While many concerns remain as genuine and applicable today as they did in 2004, there are just as many that get lost in the…clouds. The FFIEC, for example, calls for "clearly written contracts that provide sufficiently detailed assurances for performance, reliability, security, confidentiality and reporting."[79] In contrast, most cloud computing agreements (and perhaps private cloud agreements to a lesser extent) are take-it-or-leave-it documents that heavily favor the provider with robust disclaimers of warranties and limitations of liability. Other federal statutes, like FINRA's Notice on Members' Responsibilities When Outsourcing Activities to Third-Party Service Providers, issued in 2005, requires NASD members to design supervisory systems and due diligence plans that include monitoring a service provider's compliance with the terms of any agreement…and assessing such provider's fitness and ability to perform the covered activities being outsourced.[80] Even the largest and most capitalized financial services firms will think twice about cloud computing if they are required by statute, rule or guidance to audit and monitor hundreds of data centers around the world for the *cost savings* it anticipates enjoying back at home. We did say cloudy, right?

The Necessity of Teamwork – Working with Your IT Professionals To Determine the Optimal Cloud Framework

When making determinations regarding the type of cloud

environment to utilize and adopt (private, public, community or hybrid), and the applications and/or business functions that are suitable to be hosted in a cloud environment, it is essential that the financial services firm and individual lines of business look to its information security officer or director and his/her operational, compliance and legal teams for participation and guidance. When selecting a vendor, a financial services firm needs to be reasonably certain that the selected vendor has the capabilities to ensure compliance with all applicable laws and regulations that govern the firm's operations. Because cloud computing is a rapidly growing IT services sector, there is a large (and ever-expanding) pool of service providers from which to choose—including major players such as Oracle, Google and Amazon, and existing end-to-end IT infrastructure service providers that are eagerly pushing into this sector with the hope of capturing market share. While it might be tempting to leverage an existing relationship with an IT services vendor that may not have a long track-record with respect to cloud computing, the firm should be wary that it does not become a test case for such a service provider and, essentially, end up funding cloud-computing R&D. It also should be noted that, even more so than with respect to other, more established, IT services, standard terms and conditions in cloud-computing service agreements provide little in the way of customer protections and remedies. Therefore, it is critical to have strong negotiators and legal representation on these deals to ensure that the firm gets what it needs with respect to service levels, warranties, remedies, and other terms and conditions.

A Financial Institution's Preliminary Cloud-Computing Check List

Once the cloud computing project team is formed, the financial services firm needs to develop its requirements, specifications and due diligence checklist to measure the various third-party service providers. While these documents will be specific to the organizational standards, line-of-business requirements, and the specific business functions that it seeks to move into a cloud environment, the following suggestions may be helpful:

- Determine which business functions might be suitable for different cloud environments and classify your information assets by sensitivity. *For example, processes that require high-capacity processing but are utilized only periodically may benefit greatly from a cloud environment where capacity is available on-demand. On the other hand, functions that involve the collection and treatment of large amounts of NPPI may require use of a private cloud, or may not be suitable for transfer to a cloud environment at all.*
- Establish a robust and comprehensive set of requirements specific to the lines of business and specific business functions the firm would optimally operate, either partially or wholly, in a cloud environment. *It may be beneficial to develop the service level agreement in advance so that all the operational and regulatory requirements are on the table once you begin your vendor selection process. With this approach, it will quickly become apparent which vendors clearly are not able to satisfy your requirements.*
- Develop detailed and extensive governance processes and procedures, including meaningful goal-setting, policy and standard development, audit rights, frequent steering committee meetings, and clear escalation procedures.[81] *Considering the relatively nascent state of evolution of cloud computing services, it may be even more critical than with other more developed IT services, to drive the service requirements. Do not let a vendor get away with the "that's not market" approach.*
- Establish some form or protocol that allows the financial services firm to identify where its infrastructure and data are situated, both technologically and operationally. *You cannot simply launch and run your business purely on faith*.
- Consider not only the service provider's capabilities regarding robustness of information security, but also how readily your firm's information is able to be retrieved in the event of an investigation or natural disaster. *If your firm is subject to a regulatory investigation, the service provider must be able to cooperate and facilitate the investigation by providing the information required by the regulatory agency without compromising other information.*
- Adjust or develop your firm's internal policies to address the unique issues posed by the purchase and utilization of cloud computing services. *Because business owners may now, potentially, bypass IT entirely and purchase pre-packaged cloud services to perform certain tasks, the parameters around this process need to be clear.*

Conclusion

Adoption of cloud computing within the financial services industry is still in its infancy, as evidenced by a survey, carried out earlier in 2010, of several IT professionals

within financial services firm. The survey, which sought to uncover the top information technology and security priorities for today's financial services companies, found that essential IT functions, such as security and compliance, continue to be the top concern for IT departments industry-wide. The survey reported:

- 34 percent of respondents believe that cloud computing is not strategic to their company, while 26 percent of respondents believe their company is risk-averse to cloud computing
- 58 percent of respondents only plan to invest in essential IT functions, such as security and compliance
- More than 75 percent of respondents are concerned about increasing government regulation

While at first glance these statistics provide somewhat of a dark outlook for the future of cloud computing within the financial services industry, it cannot be stressed enough that these numbers likely reflect the loggerhead of this new technological paradigm pitted against an increasingly complex, confusing and perhaps ill-equipped regulatory framework within which to operate. The fact remains, however, that the financial services industry continues to be very competitive and increasingly geographically independent. More than ever, financial institutions need to be agile as they expand both their girth and their global footprint. At the same time, internal IT projects are taking longer as IT resources get stretched to the limit. In many cases, cloud computing and SaaS-based deployment models have the inherent potential to give institutions the agility they need, while freeing IT from the somewhat mundane tasks of managing infrastructure and allowing them to focus on the strategic needs of the business unit. That, however, must be coupled with the extensive and steadfast due diligence and ongoing monitoring of a cloud provider's services to ensure continued compliance with the applicable laws and regulations governing a firm's operations. When asked to explain the survey results, LogLogic[82] CEO Guy Churchward aptly summarized them as follows: "While the cloud holds many benefits for the enterprise, we're not surprised to see that financial services firms are hesitant to adopt cloud computing. There are still many lingering questions about data security and transparency in the cloud, and it's up to cloud providers to offer visibility into these practices before we see mainstream adoption from financial services firms."

Only time will tell how widely adopted cloud computing becomes within the financial services industry, but as the offering continues to mature and improve, it's likely to be too enticing a service to be left unconsumed by financial institutions large and small.

— CHAPTER 9 —

Cloud Computing in Advertising & Marketing: Looking for the Silver Lining, Making Rain

Chapter Authors

Joseph I. Rosenbaum, Partner – jrosenbaum@reedsmith.com

Keri S. Bruce, Associate – kbruce@reedsmith.com

Advances in digital wired and wireless technology are rapidly expanding both the types of media and the devices that advertising, marketing and brand professionals can use to reach consumers. Not only is the B2C landscape changing, but even B2B marketing is undergoing rapid and often radical shifts in tactics, techniques, challenges and opportunities.

Indeed, the advertising and marketing buzzwords over the past few years have shifted from "eyeballs" to "engagement"; from "brand recognition" to "brand reputation"; from "messages" to "conversations"; and from "online" to "digital," as the inclusion of wireless and mobile applications and interfaces has been transformative in ways we could never have imagined just a few years ago. With technology as a dynamic enabler, cloud computing represents yet another shift in the ability of advertisers and agencies to reach their target audience, and for consumers and businesses to interact with the marketing community.

As technology decreases in cost and increases in utility and accessibility; and as increased bandwidth and compression algorithms expand the capabilities, features and functions of interface devices, marketing professionals are increasingly able to capitalize on these technological innovations in a number of ways through: (1) an abundance of new content (music and video, for example) and programming made for online and mobile, mushrooming at an exponential rate; (2) “apps,” which are rapidly becoming the preferred method of not only essentially bookmarking favorite web locations and accessing content, but also of sharing of information on social media; (3) robust data collection—there is a marked increase in data available, shared, created and collected; and while monetization and pricing, to some extent remain confusing in the marketplace, we have never before seen such robust capability to capture advertising metrics, demographics, geographic, and context-sensitive data, as well as consumer personal information and preferences; and (4) technology scalability—spikes in server usage and bandwidth demands are more easily handled, and changes in requirements can often be responded to in seconds, not days or weeks.

Whether you are in a business that advertises, develops advertising, serves advertising, collects advertising information, measures advertising data and effectiveness, monitors advertising, or displays or distributes advertising, the real time, digital demands that can change in an instant have to put a strain on the current IT infrastructure, information security mechanisms, and existing storage and processing capacity.

In an effort to manage the load and demand issues in a rapidly changing technological environment, many companies are looking to cloud computing as a means of addressing their changing (and often increasing) IT infrastructure needs. At the same time, global companies are also looking to reduce costs and figure out the challenges of global branding, coupled with local relevance. While cost savings are certainly an initial selling point of cloud computing (just as it was with outsourcing information technology, business processes or call center requirements decades ago), moving to the cloud, in whole or in part, requires planning and management—and unfortunately, all too often the ad sales, marketing and brand management groups are not even consulted when a decision to look to cloud computing is considered or taken; it is often viewed purely as an information technology, security or compliance matter, best handled by the IT department.

Overview of Cloud Computing

While there is no industry agreed-to or standard definition, cloud computing is generally defined as Internet-based computing, where shared resources, software and information are provided to computers and other devices on demand, like a public utility. Cloud computing allows users to access hardware and software over the Internet on a pay-per-use basis through utility-like access portals, often coupling the availability of programming applications, data and content in a cloud environment as well. While ostensibly, a cloud computing model can be implemented internally by a company's own systems and communications staff, that presumably creates none of the prioritization, control and management challenges that outsourcing to a third-party cloud provider entails. For purposes of this analysis, we focus on external cloud services provided by third parties over a network connection.

There are three primary categories available as cloud computing services:

- Infrastructure as a service (IAAS): Delivers virtual servers on demand, such as Elastic Compute Cloud, available from Amazon Web Services LLC (the Amazon.com entity providing cloud services—we'll just use "Amazon")
- Platform as a service (PAAS): Delivers developmental platforms, such as Microsoft's Windows Azure AppFabric, that allow each customer to develop and run its applications
- Software as a service (SAAS): Delivers software that users can access over the Internet, such as GoogleDocs (Google's suite of word processing, presentation and spreadsheet programs), which is used over the Internet and stored on Google's servers.

For advertisers, publishers, advertising networks and agencies, there are, pardon the pun, a host of benefits to be found in cloud computing, including providing: (1) scalability; (2) collaboration capabilities; (3) ad serving options; and (4) advanced data collection capabilities.

Scalability

Cloud computing is highly scalable. Ad serving, depending on success metrics, timing and other factors, can be ramped up or reduced, with multiple iterations or variations or types of ads stored and available to be served on demand, without investing in costly infrastructure or without suffering the vagaries of IT peaks and valleys. Businesses can launch new services, or develop and implement corresponding advertising and marketing campaigns, with little concern over whether a spike in demand or views or the need to increase ad serving, will create a serious problem or even be unavailable. If an advertiser launches a new advertising campaign with a Super Bowl commercial, the cloud and its scalable capacity should generally be able to handle the resultant spike in demand with nary a peep.

Collaboration

Cloud computing also facilitates activities that are not simple or that may be resource-intensive (or unavailable) using traditional IT infrastructures. For instance, cloud computing can provide the ability to collaborate online and to access information anywhere in the world, with multiple applications, multiple access points, common content, information and data availability, in real time, across time zones and geography—all without requiring any additional resources, effort, equipment or software by anyone on the collaborative team. Removing dependence on all of these allows the advertiser to collaborate with agencies, suppliers, talent, publishing networks around the globe, as well as internally with marketing and—here it comes—legal, whether inside or outside counsel!

Cloud computing has the potential to change the way companies and industries operate. The creation of private clouds designed to reflect the unique requirements, standards, and services of a company or an industry, will proliferate. Of course, to be ubiquitous and feature-rich, they will need to interface and interoperate with other clouds; but consider that today, it remains common practice to send CDs or DVDs back and forth, or emails with links (or even attachments!), or to create FTP sites, in order to review commercials as they are being developed. Reviews may be made by creative teams, marketing, compliance, legal—all of whom may have input or may require editing before a commercial can be released, whether for network clearance or for public viewing. A cloud enables the collaboration to take place with standardized tools and techniques, auditable methodology, interactive cooperation and clearly a more cost-effective platform, reducing the overall preparation, operation and distribution expense.

Ad Serving Options

Further, and certainly not least, cloud computing offers a wider array of choices and flexibility for advertisers to distribute and display advertising. Consider the ability to create and distribute advertising that could reach consumers regardless of the technology they had

available. The cloud could detect and serve ads in a form, format and version, just right for the device the consumer is using at that very moment. Similarly, through authentication methodologies, individuals traveling or outside their home base will still be served advertising relevant to them, because the cloud will "know" the log-in credentials or the mobile device number. Traveling to Spain, you will still see ads in English targeted to you—unless of course, you tell the "cloud" you want something different.

Context-sensitive searches will allow consumers to select advertising based on their preferences, literally on a moment's notice. Visiting Amsterdam? A search for local restaurants and ads will be able to target your needs. Business meetings in Buenos Aires? Search for directions and you could see English-language ads for business services in or around town. Although all of these features may currently be available today using non-cloud platforms, make no mistake, their cost-effectiveness, universal availability, and ubiquitous functionality are meager compared with the robust capabilities that will soon be available in the cloud.

Advanced Data Collection Capabilities

Cloud computing increases the ability to gather data and analyze metrics across different platforms. The most precise data (*i.e.*, personal identifiable information about a consumer) still remains the subject of volatile and heated debate. In the cloud, global data, both aggregate and consumer-specific, will become the subject of even hotter debate. As will be noted below, privacy, surveillance and similar issues will continue to be hotly debated, but one area that everyone is likely to agree upon is the fact that cloud computing will make significantly greater amounts of valuable information—gathered on a global scale, segmented in as many ways as the marketer's imagination can conjure up—accessible and usable.

Key Legal Issues

Although myriad legal issues arise in a cloud computing environment, this paper will focus on three key areas of concern: (1) confidentiality, privacy and data protection; (2) global regulatory compliance; and (3) intellectual property.

Confidentiality, Privacy and Data Protection

One of the primary legal concerns expressed by regulators, consumer groups and information security professionals when it comes to cloud computing revolves around issues of privacy and data protection—the security, integrity and reliability of information and data. In a cloud computing environment, businesses are concerned about ceding control over their data, their proprietary processes and ultimately their digital capabilities, to a third party. Consumers search for assurances that their personally identifiable information, personal and private data, their financial and health records, for example, will be safe and secure, protected not only from unwanted and unauthorized intrusion, misappropriation and alteration, but also from use in ways that were not intended and are often unknown and undisclosed.

Information and data may be subject to laws governing their collection, processing, storage and use. Who is responsible for compliance may well depend on the relationship of the parties (is it B2B, B2C, or some combination of these) and the laws and regulations that apply (either by contract or based on the jurisdiction that applies to one or more of the parties). Multiple parties, multiple jurisdictions and the blurring of responsibility for delivering data, content, application programs, processing resources and communications, or interface capabilities, will likely give lawyers much to negotiate (and litigate) over the next decade.

From the advertisers' perspective, the "service" in a cloud will likely consist of a continuum of activities, from the creation of advertising to the delivery of the ads themselves, and ultimately to measuring the effectiveness and resultant product and service delivery when positive responses are received with respect to the advertising. Contractually allocating the risks involved at each stage of the process is likely to be something the industry struggles with for some time to come, as standards will be difficult to define and the sheer diversity of parties, roles and responsibilities with endless permutations can be numbing.

While the protection of personal and personally identifiable data and information is subject to a variety of laws and regulations in the United States and many countries around the world (*e.g.*, in the United States, the Graham-Leach-Bliley Act applies to personal information collected by financial institutions, and the Health Insurance Portability and Accountability Act to medical and health information), the advertising and marketing industries face new and uncharted challenges as the regulation of virtually all kinds of information derived from digital advertising is being targeted for legislation and regulation. Most industry professionals are all too familiar with terms such as "browser ad blocking," "opt-in" cookie legislation, "online behavioral advertising," "tracking," "location based marketing." All of these terms have arisen in the context of some technological innovation, enabling advertisers to gather more information, segment demographics more

granularly, and focus increasingly relevant advertising to the right target audience. Unfortunately, the abuses that have crept into the system have caught the attention of regulators and legislators, and it is too early to tell what, if any, beneficial effect the industry's self-regulatory initiative (i.e., the Digital Advertising Alliance and the online behavioral advertising self-regulatory guidelines), is having on these abuses.

In addition to industry regulations, most states in the United States have laws regulating the collection and security of the personal information of their residents, and states are continuing to strengthen these laws by proposing new laws or amendments to current laws. In April 2011, California introduced a bill that would require companies doing business in California to provide Internet consumers with a method to opt out of the collection or use of any "covered information." Other states have also introduced new bills relating to data collection and/or security breach requirements, including Massachusetts, Hawaii and Colorado.

Data protection laws and regulations abound throughout the world. Consider for instance the European Union's Data Protection Directive[83] ("EU Directive") that requires Member nations to enact legislation and implement regulations regarding the collection, processing, storage and transfer of personal information outside of the EU, and attaches to any personal information processed by a Member State and to personal data of residents within each Member State. This imposes restrictions on the export of personal data of EU citizens and residents to anywhere outside the EU.[84] Laws and regulations in the United States, European Union and throughout the world create a patchwork quilt of obligations, disclosure requirements, restrictions, responsibilities and liabilities that global and multinational companies will need to navigate in a cloud environment.

When it comes to security, there are laws, regulations and, increasingly, industry self-regulatory requirements (*e.g.*, the Data Security Standards of the Payment Card Industry, commonly referred to as "PCI DSS") that companies will need to comply with as consumer information is collected in connection with advertising and marketing. Encryption and data security is or will be required when, for example, personally identifiable information, credit or other payment and financial information, health and medical information, is involved.

The requirements often extend not merely to the advertiser, but also to every entity that touches the information: agencies, vendors and suppliers, distributors, networks and publishers will be required to contractually commit (or be formally subject to regulations). Due diligence, modified contract terms and conditions, and constant reevaluation is needed to ensure each of these entities has adequate physical and logical security controls for safeguarding the information and data, and is properly authenticating users; controlling who is given access to the information; who the information and data is shared with; when, where and how appropriate disclosures, opt-in or opt-out opportunities are given; and so much more, depending on the situation.

For instance, if the provider's terms of service allow the provider to have access to a user's data or to share the data, could this violate the advertiser's own privacy policy? Google's terms of service provide that Google has the right to "pre-screen, review, flag, filter, modify, refuse or remove any or all Content from any Service."[85] If an ad agency uses the services of the "cloud," would contractually agreeing to such a right violate the provisions of contracts between the agency and its client, the advertiser, or the advertiser and customers and consumers?

Should advertisers seek to add (or require that their agencies, suppliers and others add) specific clauses that prohibit cloud providers from monitoring their information and data, or using it, other than as necessary to provide the services (*e.g.*, capacity planning, network traffic monitoring, operational and systems configuration)? Consider the following. Not that long ago, in an advertising environment ruled by passive, one-way communication—television, print, radio, direct mail—only the advertiser, its agency and perhaps the retailer conducting the promotion or redeeming a coupon, would be in a position to gather personally identifiable information about consumers. Rating services and metrics were by inference and statistics, more often than not, rather than by direct observation.

Today, network publishers, ad serving networks, search engine providers, social network operators, wireless carries and even browser technology providers, are in a position to gather such data and information. Indeed, not only first-party advertisers, but third parties as well can now obtain, store, analyze and ostensibly use behavioral marketing information about consumers.

As you may already know, the U.S. Federal Trade Commission ("FTC") takes the view that a company's website policies, its terms, conditions and privacy statements—the agreements by which consumers are bound when they visit or register and use a particular website—represent claims and express representations to consumers about how their information and data will be collected, stored, used and, if applicable, shared. Failure to

adhere to one's own website statements, even if well beyond what the law requires, not only can give rise to a cause of action from a consumer alleging breach of contract, but may also draw action from the FTC for misleading or deceptive advertising under section 5 of the FTC Act.

It is likely that we will continue to see additional and/or revised regulations ahead as regulators begin to address the data privacy risks involved in cloud computing. For instance, this year the European Union is planning to propose a new general legal framework for the protection of personal data in the EU covering data processing operations in all sectors and policies of the EU.[86] We have also already seen the proposal of several new federal privacy bills.

Global Regulatory Compliance

In a cloud computing environment, a company may no longer know where its data is at any particular point in time—physically or logically; and while technically it may be possible to audit and trace each bit and byte, as a practical matter, from an availability and access viewpoint, the data might be stored on one or more servers somewhere—across the street, across state lines, national boundaries or across the globe, perhaps even in multiple data centers all over the world. Which jurisdiction's laws and regulations govern? What level of data and privacy protection is "adequate"? What about transborder data flow? Is your company subject to the laws and regulations of multiple jurisdictions, potentially dynamically changing jurisdictions? Due process and subpoena requirements are not harmonized around the globe—in some jurisdictions, law enforcement and government officials have wide-ranging power to examine and even confiscate data resident on processors or storage devices within their borders.

While a company's service agreement with its cloud provider can address choice of law between the two parties, it will not provide either a company or an individual user with a choice of where its data will be stored, where it might be routed or processed, and how it can be dealt with by others in a variety of jurisdictions. In the United States, the USA PATRIOT Act, and in the United Kingdom, the Regulation of Investigatory Powers Act, can provide government access to private data. First Amendment protections under the U.S. Constitution might not be immune from defamation, criminal or civil liability in other jurisdictions. As most advertisers already know, advertising standards and regulations vary widely across jurisdictions, and while we tend to think it is only where the ad is "displayed" or visible that laws and regulations would really apply, that is a notion borne more in common sense than legal or regulatory precedent. Newsweek.com moved its website to a cloud provider.[87] The *Chicago Sun Times* is deploying its editorial software in a cloud computing environment.[88] Are journalists and is news-content accorded the same protections everywhere? In a cloud environment, that is not a trivial question.

What if the intellectual property laws in one or more nations provide little or no protection? What if your data and information is passing through, enroute to its destination, but transmitted through servers and repeaters and transmission mechanism in multiple jurisdictions? Imagine having a telephone conversation between individuals in country A and country C, but the signal passes through country B on its way. What if country B has no protections against wiretapping? Against listening in on the conversation? Against taking the contents of the call and using it within country B? What if country B has laws that prohibit, restrict or object to content transmitted across its borders for any number of reasons? Serving advertising is not that different from serving any other content, and if a country has the capability and the right to censor or restrict one, it can do so with any content, including advertising. Right now some cloud providers, such as Amazon's EC2 Service, have ways to address this by allowing users to select "Availability Zones." Amazon currently has multiple availability zones in the United States and Europe.[89] While of some comfort, an "Availability Zone" is still not dispositive of the route personally identifiable, trade secret or sensitive health or financial information may take on its way from point A to B!

The situation is indeed cloudy and it may take quite some time before we can see clearly and before cloud users have the ability to manage these issues with less risk than is evident today.

Intellectual Property

Although intellectual property issues associated with Internet-based technologies are not new, cloud computing adds an interesting twist, and we have already mentioned a number of them above. Because of the multi-tenancy and quasi-public nature of cloud computing, a company could theoretically be putting its trade secrets at risk by storing its proprietary and sensitive advertising, development, and creative, as well as advertising metrics, with a cloud provider. What if the cloud service agreement allows the cloud provider to see, scan or use the company's information in some way? Are you required to perform adequate due diligence on the security, integrity and reliability of cloud providers, their data and information

security standards, privacy policies, compliance mechanisms? Could you be liable for failing to make reasonable inquiries and obtain contractual covenants in these areas? After all, cloud providers are not immune to security breaches. In 2009, the Electronic Privacy Information Center (EPIC) filed a complaint with the FTC seeking an investigation into Google's cloud computing services after there was a security breach in Google Docs.[90]

Conclusion

Cloud computing holds significant promise for the advertising, media, gaming and entertainment industries. But make no mistake: there are challenges and concerns that must be carefully considered—evaluated based on the nature of the activities, data and information, and requirements. For advertisers, agencies, network and publishing providers, the decision to go to the cloud should be made carefully, taking into account these factors and weighing the benefits and risks. While the technology and the regulatory landscape of cloud computing is and likely will continue to change dynamically in the months and years ahead, cloud computing, like any innovation, can represent extraordinary risks and potential new liabilities, but may also provide a host of benefits and a promise of increasingly globally effective, locally relevant, readily distributable, inexpensive delivery of high-quality advertising in the future.

— CHAPTER 10 —

Health Care in the Cloud – Think You Are Doing Fine on Cloud Nine? Hey, You! Think Again. Better Get Off of My Cloud.

Chapter Authors[91]

Vicky G. Gormanly, Associate – vgormanly@reedsmith.com

Joseph I. Rosenbaum, Partner – jrosenbaum@reedsmith.com

Introduction

The interest level in storing health records in digital format has grown rapidly with the lower cost and greater availability and reliability of interoperable storage mechanisms and devices. Health care providers like hospitals and health systems, physician practices, and health insurance companies are among those most likely to be considering a cloud-based solution for the storage of patient-related health information. While lower cost, ubiquitous 24/7 availability, and reliability are key drivers pushing health care providers and insurers to the cloud, a number of serious legal and regulatory issues should be considered before releasing sensitive patient data into the cloud. This article seeks to highlight some of those concerns and considerations.

An important first step for any health care provider considering retaining the services of a cloud services provider, and ultimately moving data, programs or processing capability to a cloud environment, is to determine precisely what services are contemplated to be used. Depending on the services that are involved, certain provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") will be implicated. This article will highlight areas of consideration for health care providers who are exploring the possibility of engaging the services of a cloud services provider and moving some or all of patients' health records or other sensitive medical information to a cloud.

The Basics of Health Information Privacy

HIPAA's goals, as stated in the statute's introductory text, are "to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes."[92] This multitude of aspirations gave rise to the Administrative Simplification Regulations (the "Regulations"), which set forth a system for handling health data.[93] The Regulations, which are lengthy and complex, include the Privacy Rule, the Security Rule and the Enforcement Rule.[94]

In 2009, HIPAA's requirements were augmented by the Health Information Technology for Economic and Clinical Health Act ("HITECH"),[95] which was adopted as part of the American Recovery and Reinvestment Act in 2009. Among other things, HITECH expands the scope of civil and criminal liability for violations of the Privacy and Security Rules, and increases civil monetary penalties applicable to a violation. Further complicating matters, many state legislatures have added a layer of state regulation to the federally mandated requirements. Because of the wide reach of HIPAA and the multitude of players subject to its provisions, health care providers who decide to use a cloud-based system to store and manipulate data must give due consideration to HIPAA and its implementing regulations.

Cloud Services Providers and HIPAA

HIPAA extends only to "protected health information" ("PHI"), which is "individually identifiable health information that is transmitted by electronic media; maintained in

electronic media; or transmitted or maintained in any other form or medium."[96] "Individually identifiable health information" is "information, including demographic data, that is created or received by a health care provider, health plan, employer, or health care clearinghouse, and relates to: (i) the individual's past, present or future physical or mental health or condition; (ii) the provision of health care to that individual; or (iii) the past, present or future payment for the provision of health care to the individual and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual."[97]

By statute, two types of entities are subject to HIPAA—covered entities and business associates. A "covered entity" is a (i) health plan; (ii) health care clearinghouse; or (iii) health care provider who transmits any health information in an electronic form in connection with a transaction covered by HIPAA.[98] Therefore, unlike most health care providers, a cloud services provider would not likely be considered a "covered entity" under HIPAA.

However, what is not clear is whether, under what circumstances, and to what extent, a cloud services provider would be considered a business associate. Generally, a "business associate" is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides services to, a covered entity that involves the use or disclosure of individually identifiable health information.[99] HITECH expanded the definition of "business associate." In July 2010, the agency charged with enforcement of the Privacy and Security Rules, the Office for Civil Rights ("OCR"), issued a proposed rule implementing certain provisions of HITECH. The proposed rule modified the definition of "business associate" to include, to some degree, subcontractors who are merely "downstream entities."[100] Sanctions for HIPAA violations have been broadened accordingly; a violation of an applicable requirement by a downstream entity will leave that entity directly liable for civil penalties.

Business Associate Status

Under HIPAA, as modified by HITECH, business associates are, among other things, directly responsible for: (i) establishing administrative and technical safeguards applicable to PHI, including limiting access to facilities housing such information; (ii) designating a privacy officer; (iii) developing an information privacy and security plan; (iv) providing notice of privacy practices; and (v) providing accountings of disclosures, as well as notices of unauthorized uses or disclosures of information. Thus, it is crucial for health care providers to determine whether services contemplated by the use of a cloud services provider would give rise to a "business associate" relationship.

Generally, the Regulations require a covered entity to have a contract or other arrangement in place with its business associates, such that the business associate provides satisfactory assurances it will appropriately safeguard any and all PHI that it receives, creates, maintains, or transmits on behalf of the covered entity. In light of this requirement, covered entities and business associates frequently demand that any contractor who even remotely does or might come into contact with that covered entity's PHI, sign a business associate agreement. Cloud services providers are no exception to this general assertion.[101]

That said, whether the services provided by a cloud services provider render it a business associate is not always clear, and recently has developed into a topic of much debate.[102] A cloud services provider's status with respect to a health care provider may depend on the type and degree of services it provides. Business associate "functions or activities" can include claims-processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and re-pricing of claims. To the extent a cloud services provider performs these services, it would appear that a business associate relationship exists.

In the proposed rule promulgated last July, the OCR advised that it considers persons or entities that *facilitate the transmission of data* to be business associates.[103] When a "downstream entity" contracts with a business associate, the parties must adhere to the Privacy and Security Rules to the extent that they require access to PHI.[104] Alternatively, "data transmission organizations that do not require access to protected health information on a routine basis would not be treated as business associates," nor are "entities that act as mere conduits for the transport of protected health information but do not access the information other than on a random or infrequent basis."[105]

Therefore, in order for a health care provider to determine what, if any, HIPAA implications exist with respect to its use of cloud-based services, a factual analysis must be performed of the precise services that are contemplated. Specifically, a health care provider needs to consider whether and to what degree a proposed cloud services provider will need to have access to PHI in order to provide its services. If access to PHI is required to perform the services, the form and format of the data must be examined (*e.g.*, if the data is de-identified, its use will not

be restricted[106]). The unfortunate implication, therefore, is that it is not possible to reach a broad or general conclusion that a cloud services provider will always or never be subject to HIPAA. What can be determined is whether a specific service, consisting of specific activities, with access or use of specific health or other medical records and information, is or is not subject to HIPAA.

The Health Care Industry and HIPAA Demands

The highly regulated health care industry broadly includes hospitals, skilled nursing and long-term care facilities, specialty and primary care physicians and other health care professionals, insurers, pharmacists, software services providers, and last, but certainly not least, patients. With the impetus of government-paid incentives to adopt and meaningfully use electronic health records ("EHRs"), the use and sheer volume of EHRs is rapidly increasing. In addition, patients are increasingly being given the opportunity to create a web-based personal health record.[107] It is inevitable that some of this data will be stored in the cloud.

When considering engaging the services of a cloud services provider, the health care provider must take into account several characteristics and requirements of electronic and/or personal health record systems, including (i) interoperability; (ii) security requirements; and (iii) storage, access and reporting needs, for internal management, audit and compliance purposes. HIPAA covered entities should explore and evaluate a potential services provider's understanding of, and ability to support, the covered entity's unique regulatory needs and obligations. These abilities range from the obvious—maintaining data in a secure manner (*e.g.*, by the use of encryption)—to the less obvious, such as providing the covered entity with the ability to parse out data so that it can meet reporting or notification requirements, and allow it to account for uses and disclosures of PHI.

Interoperability

If the desire by health care industry players to implement an EHR system has one overarching theme, it is the tremendous benefit of having the same information available across the full health care continuum—from primary care providers to specialists; from surgeons to pharmacies; from insurers to patients. To realize this benefit, EHRs and the systems in which they are stored must be interoperable[108]—in other words, the systems must be able to "talk" to each other and exchange information, preferably quickly, accurately and seamlessly. Balancing interoperability with privacy is, therefore, an important consideration for health care providers who will increasingly require cloud services providers to have the demonstrated capability to offer a storage system that is able to communicate and exchange data with other systems, without compromising data security, in compliance with all legal and regulatory requirements.

Security

HIPAA's Security Rule sets forth in specific detail requirements for the physical, technical and administrative safeguards for PHI that is stored electronically.[109] Examples of these requirements include imposing physical limitations on access to data, implementing physical safeguards for workstations[110] that access the data, and providing protection against threats or hazards to the security or integrity of the information. Health care providers should evaluate prospective cloud services providers in light of these requirements in order to determine whether the cloud services provider understands the requirements and will be able to comply.

Storage and Access

The manner in which data will be stored and accessed is another concern for health care providers. Under HIPAA, individuals have the right, with some limitation, to seek access to their information and to authorize its use and disclosure by others. Specifically, the Privacy Rule sets forth the manner in which use and disclosure of health information may be authorized. Because of these requirements, health care providers should ensure that a potential cloud services provider has a system in place that allows for personal authorization of access to information. Health care providers who transfer these authorizations to an electronic format need to be able to electronically associate an authorization with the particular data that a patient is seeking to share. Most importantly, health care providers must ensure that no other data is released other than that data specifically authorized.

Additionally, health care providers need the ability to keep track of these personal authorizations, as well as unauthorized disclosures of PHI.[111] The Privacy Rule, as amended by HITECH, requires covered entities to make available, upon the request of an individual, an accounting of certain disclosures, including unauthorized disclosures, of the individual's PHI through an "electronic health record."[112] The individual has a right to request an accounting of disclosures that occurred during the three years prior to the request.[113] The type of data to be presented in such an accounting is set forth in the Privacy Rule. Although the regulatory interpretation of the manner in which electronic data is to be collected and presented is in flux, health care providers need to confirm that they will

have the ability to access this data in a particular format. In light of the potential for future changes, a cloud-based system should be as flexible as possible.

Conclusion

Cloud computing presents a huge potential for hospitals, health systems, physicians and even health insurers to obtain and maintain cost-effective EHRs. Indeed, cloud computing, if implemented in accordance with legal and regulatory requirements, can help assure that the patient is able to receive high quality health and medical care by correspondingly assuring that those responsible for the delivery and application of that care have timely, accurate and complete information, protected from alteration or file record corruption, and protected from inappropriate or improper disclosure. Web-based applications have many attractive and powerful features that allow for a productive exchange of health information and, consequently, better care for patients across the continuum of services. As this article and our experience have shown, numerous important legal and regulatory implications are related to the use of EHR, the storage of PHI and the "digitization" of health and medical information. Health care providers subject to HIPAA should give great attention to these implications, and carefully consider the risks associated with using cloud-based services for the operation and delivery of health and medical services.

— Biographies of Authors and Editors —

Joseph I. Rosenbaum, Partner and Chair, Advertising Technology & Media Law Group
New York · +1 212 702 1303 · jrosenbaum@reedsmith.com
Blog: www.LegalBytes.com

Joe chairs Reed Smith's global Advertising Technology & Media Law practice, and has more than 30 years of international experience across a wide range of sophisticated and complex commercial transactions, in industries including advertising, entertainment and media, financial services, travel-related services, technology and many more. Joe specializes in the law and policy arising at the intersection of technology and online and behavioral advertising, social media, entertainment, finance, e-commerce, information security and digital rights, online gaming, promotions, privacy and data protection, among others. Joe's experience includes virtual worlds, mobile marketing, digital payments and PCI compliance, digital broadcasting, co-branded credit and gift cards, loyalty rewards programs, branded entertainment, online product placement and endorsements, user-generated content, buzz, word-of-mouth and viral marketing, licensing, software development and outsourcing. Joe lectures and writes extensively and, among others, has authored a book on outsourcing (*Outsourcing Agreements Line by Line*; Aspatore Publishing, 2004) and a seminal law journal article on privacy ("Privacy on the Internet: Whose Information Is It Anyway?"; *Jurimetrics Law Journal*, 1998). Joe's work has been cited by appellate courts, law reviews and journals, industry and trade periodicals. Joe is regularly quoted in widely respected publications such as the *National Law Journal*, Advertising Age, the American Banker, Euromoney and has been interviewed and appeared as a commentator on CNBC's *Squawkbox* and CNN Financial's *Business Unusual*. Joe is General Counsel & Secretary to the Interactive Advertising Bureau and a member of the Advisory Board of the Center for Law, Science and Technology at the Sandra Day O'Connor College of Law at ASU.

Leonard A. Bernstein, Partner – Philadelphia +1 215 851 8143 · lbernstein@reedsmith.com

Len is a member of the Financial Industry Group and a member of Financial Services Regulatory Group. Len founded and chairs the firm's Financial Services Regulatory Group and concentrates his practice in the representation of banks, thrifts, mortgage bankers and finance companies in providing consumer credit compliance advice on federal, Pennsylvania and New Jersey laws and regulations. The FSR Group addresses credit card, auto finance, deposit, residential mortgage and other retail finance products. Len is nationally known for expertise with federal Truth-in-Lending Act, Real Estate Settlement Procedures Act and similar laws, and works regularly with federal and state financial services regulators. He and his colleagues also defend class actions and individual claims filed against financial services providers. Len is also active with the firm's Financial Services Litigation defense group and has been elected to the American College of Consumer Financial Services Attorneys.

Keri S. Bruce, Associate – New York +1 212 549 0220 · kbruce@reedsmith.com

Keri is a member of the Advertising, Technology & Media group. Keri represents advertisers, advertising agencies, media companies, talent payroll companies and trade associations on a wide range of advertising, promotion, marketing, technology and entertainment matters. Her practice includes drafting and negotiating a wide variety of complex agreements including agency-client agreements, celebrity endorsement contracts, media buying agreements, sponsorships, releases, design and consulting agreements, website terms and conditions and privacy policies. She also counsels clients on advertising copy and claim substantiation, gift cards, sweepstakes, promotions and general intellectual property issues. Prior to becoming an attorney, Keri spent seven years in the advertising industry working with both technology start-up companies as well as established companies, including Palm Bay Imports, Proctor & Gamble and Ernst & Young.

Lorraine Mullings Campos, Partner – Washington D.C. +1 202 414 9386 · lcampos@reedsmith.com

Lorraine's practice focuses on assisting clients with a variety of issues related to government contracts, government ethics, campaign finance, and lobbying laws. She has particular experience in counseling clients regarding Federal Supply Schedules, creating company ethics and compliance programs related to doing business with the Federal government, conducting internal investigations, drafting and negotiating government contracts and subcontracts, and facilitating government contract compliance training. She also counsels clients on bid protest matters, federal grant programs, federal audits, and the application of the Federal Acquisition Regulation ("FAR") and individual agency supplement procurement regulations.

Claire N. Covington, Associate – Chicago +1 312 207 6504 · ccovington@reedsmith.com

Claire is a member of the Midwest Commercial Litigation Group, practicing in the area of product liability litigation. In addition, Claire serves as E-Discovery Counsel to one of the firm's major clients, a Fortune 50 company. She has experience counseling clients about a variety of E-Discovery topics, which include document retention issues, litigation hold issues and email retention issues. Claire also has experience with the issues arising out of the incompatibility of United States discovery practice with the European Union Directive on Data Privacy.

Jennifer Yule DePriest, Partner – Chicago +1 312 207 6444 · jdepriest@reedsmith.com

Jennifer is a litigator who focuses on intellectual property disputes involving patents, copyrights, trade secrets, trademarks and unfair competition under the Lanham Act. Jennifer has also successfully handled numerous complex commercial litigation matters, at the trial court level and on appeal, involving securities fraud, breach of contract, tortious interference, breach of fiduciary duty, and shareholder and member/manager disputes.

Jeremy D. Feinstein, Partner – Pittsburgh +1 412 288 7972 · jfeinstein@reedsmith.com

Jeremy is a trial lawyer with a focus on antitrust, RICO, unfair competition, business tort, and civil class action matters. He has handled major matters, both civil and criminal, for health insurance companies, financial services corporations, long-term care facilities, medical device manufacturers, and universities. His trial experience includes cases concerning monopolization, tying, and predatory pricing, lender liability, food safety, foster care and election law. He was named a "Pennsylvania Rising Star" by *Pennsylvania Super Lawyers* in 2006.

Thomas Fischl, Counsel – Munich +49 (0)89 20304 178 · jfischl@reedsmith.com

Thomas is counsel in the European Corporate Group in Munich and part of the Media & Technology Team. He provides comprehensive legal advice to mid-sized and major IT providers and companies in both the domestic and international markets, within the scope of IT law. His particular experience covers drafting and negotiating contracts covering software, IT projects, and distribution, as well as outsourcing projects. In addition, Thomas specializes in data protection law and intellectual property protection. He also serves as legal counsel in project crises and asserts his clients' interests in court. His clients include not only software and technology companies, but also clients from such industries as mechanical engineering, automotive, marketing, financial services and health care.

Stephanie E. Giese, Associate – Washington D.C. +1 202 414 9246 · sgiese@reedsmith.com

Stephanie counsels clients in matters involving federal government contracts and international trade. With regard to her federal government contracts practice, she advises high-technology clients in government and commercial contract transactions, federal grants and related litigation. Her experience includes advising federal government contractors on matters which involve claims, cost recovery and accounting, contract and subcontract administration, and rights in technical data. Stephanie advises clients regarding virtually every principal defense and civilian agency, the Department of Defense (DoD) (including all three Departments and the Defense Contract Audit Agency (DCAA)), the Intelligence Community, Department of Justice (DoJ), General Services Administration (GSA), National Aeronautics and Space Administration (NASA), National Institutes of Health (NIH), Department of Transportation (DoT), Department of Homeland Security (DHS), Department of Energy (DoE) and the Environmental Protection Agency (EPA). With regard to international trade, Stephanie's practice includes resolving export control, sanction and embargo issues subject to the jurisdiction of the U.S. Departments of Commerce, State and Treasury. In particular, she advises high-technology clients regarding obtaining export authorization and developing export control compliance programs. She also conducts internal investigations and prepares voluntary disclosures on behalf of clients.

Vicky G. Gormanly, Associate – Washington, D.C. +1 202 414 9277 · vgormanly@reedsmith.com

Michael joined Reed Smith in March 2007 and is a member of the firm's State Tax Group. Michael's practice emphasizes state tax planning in connection with business transactions, including advising public and private companies with respect to tax-free reorganizations and taxable acquisitions and state and local transfer taxes. He also handles state tax controversy matters with a particular focus on income tax and apportionment issues. In addition, Michael counsels clients on issues relating to their financial accounting provisions for state taxes.

Michael A. Jacobs, Partner – Philadelphia +1 215 851 8868 · mjacobs@reedsmith.com

Michael joined Reed Smith in March 2007 and is a member of the firm's State Tax Group. Michael's practice emphasizes state tax planning in connection with business transactions, including advising public and private companies with respect to tax-free reorganizations and taxable acquisitions and state and local transfer taxes. He also handles state tax controversy matters with a particular focus on income tax and apportionment issues. In addition, Michael counsels clients on issues relating to their financial accounting provisions for state taxes.

Joelle E.K. Laszlo, Associate – Washington D.C. +1 202 414 9212 · jlaszlo@reedsmith.com

Joelle is an associate in Reed Smith's Washington, D.C., office and is a member of the Global Regulatory Enforcement Group. Joelle's practice involves assisting clients with a variety of issues relating to contracting requirements in Federal procurements, including the applicability and interpretation of Federal Acquisition Regulation contract clauses, and the award of Government contracts. Joelle has represented clients in bid protest actions before the Government Accountability Office and the U.S. Court of Federal Claims. She also has experience advising clients on export compliance issues, campaign finance and lobbying laws, and Federal anti-trust investigations.

Richard P. Lewis, Partner – New York +1 212 205 6063 · rlewis@reedsmith.com

Richard has experience litigating a wide variety of first- and third-party insurance coverage issues. He also has experience in international arbitrations, assisting policyholders in securing coverage under Bermuda forms. Richard frequently speaks and writes on insurance coverage issues. He is a Member of the faculty of the Practising Law Institute, focusing on property and business interruption issues. In addition, he co-authored the book "Business Income Insurance Disputes," (Aspen 2006).

Rauer L. Meyer, Partner – Los Angeles +1 213 457 8124 · rlmeyer@reedsmith.com

Rauer's practice focuses on deals for the development, protection, licensing, and other commercialization of information technology (IT), web-based services, cleantech, and other technologies, and the manufacture, procurement and distribution of technology products and services. This includes negotiating and drafting complex outsourcing transactions and other IT procurement and licensing deals. His internet transactions experience includes web site development, hosting, and maintenance arrangements, co-marketing, content acquisition, and customer sale transactions. Rauer also advises clients in franchising goods and services through networks of retail, operations. This includes designing franchise systems, compliance with state and federal laws regulating sale, termination and changes of franchises, and agreement and disclosure documentation, as well as the legitimate avoidance of the franchise laws where appropriate.

Kelley C. Miller, Associate – Philadelphia +1 215 851 8855 · kmiller@reedsmith.com

Kelley Miller joined Reed Smith in January 2010 and is a member of the firm's State Tax Group. Kelley's practice concentrates on state tax planning and federal tax matters. She also handles state tax controversy matters involving income and sales and use taxes. Prior to joining Reed Smith, Kelley practiced with the federal and state tax groups of a large Washington, D.C. law firm and served as Law Clerk to The Hon. Stanley J. Goldberg of the United States Tax Court in Washington, D.C. A graduate of Georgetown Law Center (LL.M. in Taxation), she is presently the 2010 Jack S. Nolan Fellow of the American Bar Association's Section on Taxation.

Carolyn H. Rosenberg, Partner – Chicago +1 312 207 6472 · crosenberg@reedsmith.com

Carolyn frequently advises corporations, directors and officers, risk managers, insurance brokers, lawyers and other professionals on insurance coverage, corporate indemnification, and litigation matters nationwide and internationally. Carolyn also assists clients in evaluating insurance coverage and other protections when negotiating transactions and represents them in resolving coverage disputes. In addition, Carolyn is a member of the Social and Digital Media Task Force. She authored the Insurance Recovery chapter of the Social Media White Paper entitled "A Legal Guide to the Commercial Risks and Rewards of the Social Media Phenomenon." She is on the firm's Executive Committee, is Chair of the Audit Committee, and also serves on the firm's Talent Committee. Carolyn was selected by Corporate Board Member magazine as one of the country's 12 Legal Superstars and the top D&O liability insurance lawyer in August 2001 and was confirmed as the nation's top D&O liability insurance lawyer by Corporate Board Member magazine in a feature on superstar corporate attorneys in July 2004. In addition, Carolyn has been recognized by Chambers USA 2008-2010: America's Leading Lawyers for Business.

Katharina A. Weimer, Associate – Munich +49 (0)89 20304 160 · kweimer@reedsmith.com

Katharina is a member of the European Corporate Group and specialises in the area of Advertising Technology & Media (ATM). She is a commercial lawyer with a strong focus on all media- and entertainment-related matters. Among her clients are international broadcasters as well as new and old media enterprises. She also has substantial experience in copyright-related contentious and non-contentious matters, international and national data protection matters, and all aspects of doing business on the Internet. Katharina's main focus is supplemented by continuous advice in life sciences and clinical trial projects, involvement in various international transactions and litigation, and extensive experience in agreements for the virtual world.

— Endnotes —

[1] Often incorrectly referred to as "Clouds,", the song "Both Sides, Now" was a song written by Joni Mitchell that appeared on her album Clouds, released in 1969. One of her best-known songs, and inspired by a passage in Henderson the Rain King by Saul Bellow, it actually achieved popularity and wide critical acclaim after Ms. Mitchell wrote the song in 1968, when Judy Collins made the first commercially released recording and won a 1968 Grammy Award for Best Folk Performance.

[2] "Clouds in 2010: Vendor Optimism Meets Enterprise Realities, Yankee Group Research, Inc.

[3] Executive Office of the President, Budget of the U.S. Government, Fiscal Year 2011 (Feb. 1, 2010), available at http://www.gpo.gov/fdsys/pkg/BUDGET-2011-BUD/pdf/BUDGET-2011-BUD-4.pdf

[4] *See id.* at 42, *available at* http://www.gpo.gov/fdsys/pkg/BUDGET-2011-BUD/pdf/BUDGET-2011-BUD-4.pdf ("the Administration will continue to roll out less intensive and less expensive cloud-computing technologies; reduce the number and cost of Federal data centers; and work with agencies to reduce the time and effort required to acquire IT, improve the alignment of technology acquisitions with agency needs, and hold providers of IT goods and services accountable for their performance"); *see also* EXECUTIVE OFFICE OF THE PRESIDENT, ANALYTICAL PERSPECTIVES, BUDGET OF THE U.S. GOVERNMENT, FISCAL YEAR 2011 at 321 (Feb. 1, 2010), *available at* http://www.gpo.gov/fdsys/pkg/BUDGET-2011-PER/pdf/BUDGET-2011-PER.pdf ("Adoption of a cloud computing model is a major part of the strategy to achieve efficient and effective IT").

[5] *See, e.g.*, EXECUTIVE OFFICE OF THE PRESIDENT, ANALYTICAL PERSPECTIVES, BUDGET OF THE U.S. GOVERNMENT, FISCAL YEAR 2010 at 158 (Feb. 26, 2009), *available at* http://www.gpoaccess.gov/usbudget/fy10/pdf/spec.pdf ("Initial [cloud computing] pilots conducted in collaboration with Federal agencies will serve as test beds to demonstrate capabilities, including appropriate security and privacy protection at or exceeding current best practices, developing standards, gathering data, and benchmarking costs and performance. The pilots will evolve into migrations of major agency capabilities from agency computing platforms to base agency IT processes and data in the cloud.").

[6] Peter Mell and Tim Grance, Nat'l Inst. of Standards and Tech., The NIST Definition of Cloud Computing (2009), *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf .

[7] Vivek Kundra, U.S. Chief Info. Officer, Exec. Office of the President, Press Conference: In the Cloud (Sept. 15, 2009), *available at* http://www.whitehouse.gov/blog/streaming-at-100-in-the-cloud/.

[8] *See* U.S. Gen. Servs. Admin., Apps.gov, https://www.apps.gov/cloud/advantage/main/start_page.do (last visited Apr. 14, 2010).

[9] *See* Mell and Grance, *supra* note 4.

[10] This is also why Apps.gov represents a hybrid cloud. While the website itself technically is not a cloud, the capabilities that are and will be offered through it span the complete range of cloud models.

[11] All vendors seeking to offer their commercial products and services through Apps.gov must be part of GSA's Schedule 70 (Information Technology). The process for soliciting a Schedule 70 contract is detailed on the GSA's website (see, for example, http://www.gsa.gov/gettingonschedule) and will not be reviewed here, nor will the unique procedures applicable to Schedule-based procurements. Reed Smith's Government Contracts & Grants attorneys are available to assist with any aspect of GSA's Scheduling process and procurement.

[12] Available at http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

[13] *See* U.S. Gen. Servs. Admin., Frequently Asked Questions, https://apps.gov/cloud/advantage/main/start_page.do (follow "Cloud FAQs" hyperlink) (last visited Apr. 14, 2010) [hereinafter *GSA FAQs*].

[14] *See, e.g.,* J. Nicholas Hoover, "GSA to Update Cloud Computing Web Site," INFORMATIONWEEK, Mar. 24, 2010, *available at* http://www.informationweek.com/news/government/cloud-saas/showArticle.jhtml?articleID=224200193.

[15] See GSA FAQs, supra note 11.

[16] *See* Hoover, *supra* note 11.

[17] Available at http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf.

[18] *See, e.g.,* J. Nicholas Hoover, "GSA Outlines U.S. Government's Cloud Computing Requirements," INFORMATIONWEEK, Aug. 3, 2009, *available at* http://www.informationweek.com/news/government/cloud-saas/showArticle.jhtml?articleID=218900541.

[19] Thus a provider of social media applications does not need to obtain a Schedule 70 contract, or any contract, before requesting to offer its products through Apps.gov. *See GSA FAQs*, *supra* note 11.

[20] *See* U.S. Gen. Servs. Admin., Vendor Frequently Asked Questions, https://apps.gov/cloud/advantage/main/start_page.do (follow "Vendor FAQs" hyperlink) (last visited Apr. 14, 2010).

[21] See https://forum.webcontent.gov/resource/resmgr/model_amendment_to_tos_for_g.pdf.

[22] *See, e.g.*, Eric Chabrow, "DISA's Cloud Computing Initiatives," GOVERNMENT INFORMATION SECURITY, May 27, 2009, *available at* http://govinfosecurity.com/articles.php?art_id+1493&rf=03231eg.

[23] See, e.g., id.

[24] *See* Intl. Bus. Mach., Ctr. for the Bus. of Gov't, Cloud Computing in Government 26 (2009), http://www.businessofgovernment.org.

[25] See id.

[26] *See* Warren Suss, "5 Lessons from DoD's Cloud Computing Efforts," GOVERNMENT COMPUTER NEWS, Sept. 23, 2009, *available at* http://gcn.com/articles/2009/09/28/warren-suss-5-lessons-of-dod-cloud-computing.aspx.

[27] *See* Jill R. Aitoro, "DISA to Offer On-Demand Computing in 2009," NEXTGOV, July 11, 2008, *available at* http://www.nextgov.com/nextgov/ng_20080711_1829.php.

[28] See id.

[29] See id.

[30] *See, e.g.*, Elizabeth Moltabano, "Navy Awards $1.75 Billion IT Contracts," INFORMATIONWEEK, Mar. 8, 2010. *available at* http://www.informationweek.com/news/government/enterprise-architecture/showArticle.jhtml?articleID=223200156.

[31] See id.

[32] *See, e.g.*, Interview by Katie Couric, CBS News, with Robert Gates, U.S. Sec'y of Def. (Apr. 22, 2009), *excerpted in* "DoD Gates: We're Always Under Cyberattack," TECH NEWS, *available at* http://news.zdnet.com/2100-9595_22-290770.html.

[33] See, e.g., id.

[34] *See, e.g.*, Chabrow, *supra* note 20.

[35] See, e.g., id.

[36] *See, e.g.*, Matthew Weigelt, "Contract Rules Need IT Security Standards, Official Says," FEDERAL COMPUTER WEEK, April 13, 2010, *available at* http://fcw.com/articles/2010/04/13/fdcc-contract-language-gao.asp. The FDCC is a White House initiative that gave agencies a minimum set of standards for protecting their desktop and laptop computers from cyber threats.

[37] *See, e.g.*, NetSuite Inc. and OpenAir, Inc., Press Release: OpenAir Expands Research into Government Services Market (Feb. 25, 2009), *available at* http://www.openair.com/News/211.

[38] See, e.g., id.

[39] "VentureCount Launches New Cloud Accounting Solution for Government Contractors," MARKET WIRE, October 2009, *available at* http://findarticles.com/p/articles/mi_pwwi/is_200910/ai_n39260187/.

[40] See id.

[41] *See* the "Privacy and Security Safeguards" clause at 48 C.F.R. § 52.239-1.

[42] *See, e.g.*, DCAA Contract Audit Manual § 3-104.11.

[43] *See, e.g.*, the Cost Principles at 48 C.F.R. § 31 and the Cost Accounting Standards at 48 C.F.R., Chapter 99, which apply to certain federal government contracts.

[44] *See* 48 C.F.R. §§ 4.7 – 4.8.

[45] Hawaii imposes a tax similar to a sales tax on businesses.

[46] Kentucky HB 347 (Ch. 73, Acts of 2009, signed March 24, 2009); North Carolina State Laws 2009-451; Washington Engrossed Substitute HB 2075 (Ch. 535, Laws 2009, signed May 19, 2009); Wisconsin Act 2.

[47] Washington Engrossed Substitute HB 2075 (Ch. 535, Laws 2009, signed May 19, 2009).

[48] A public cloud, where data of multiple customers is hosted in a shared environment offering significant economies of scale, is appropriate for non-business critical applications that do not involve core processes, such as the archiving of non-critical data, disaster recovery, and HR. A

private cloud, involving dedicated computing environments, is preferred where the quality of service and reliability are critical. Hybrid models combine public and private clouds for a given customer. A development project in which you are merely building and testing a new app with no time sensitivity could be rescheduled and doesn't suffer mightily from an outage; it is appropriate for the public cloud. If on the other hand your data is sensitive to privacy concerns, don't send it to a public cloud, but instead to a private cloud with dedicated servers, or keep it in your data center.

[49] For purposes of this article, "data" and "information" are used interchangeably.

[50] The process of identifying, preserving, collecting, reviewing and producing ESI is referred to as e-discovery.

[51] Once a party reasonably anticipates becoming involved in litigation, the party must take appropriate steps to preserve relevant information. Federal Rule 26(b)(1) provides: "Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any non-privileged matter that is relevant to any party's claim or defense…. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence."

[52] The 2006 amendments affected Federal Rule of Civil Procedure Nos. 16, 26, 33, 34, 37 and 45.

[53] Rule 34 obligates a party to produce or permit inspection of any "designated documents or electronically stored information—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form." The advisory committee notes clarify that "[t]he Rule covers—either as documents or as electronically stored information—information 'stored in any medium,' to encompass future developments in computer technology" and that the Rule "is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes or developments." Fed. R. Civ. P. 34 advisory committee's notes (2006 amendments).

[54] *Pension Committee v. Banc of America Securities, LLC,* No. 05 Civ. 9016 (SAS), 2010 WL 184312, at *1 (S.D.N.Y. Jan. 15, 2010).

[55] *See* Rule 26(f)(3). Some jurisdictions have enacted rules that specifically require detailed knowledge of data identification, preservation and collection issues for purposes of the initial Rule 26(f) conference. For example, the Seventh Circuit recently implemented an e-discovery pilot program, the purpose of which is to evaluate and improve pretrial litigation procedures in the hopes of reducing the cost and burden of e-discovery consistent with Rule 1 of the Federal Rules of Civil Procedure. The pilot program committee created a set of principles that will eventually be incorporated into a standing order in the Seventh Circuit, to address commonly encountered e-discovery issues such as education, costs, preservation, collection and processing of ESI. Co-author Claire Covington, of Reed Smith's Chicago office, serves as a member of the Seventh Circuit's pilot program committee.

[56] Data mapping is a process that involves identifying the location of data across a company's network, or outside the network, to the extent data-hosting is outsourced.

[57] Data security and privacy issues are generally beyond the scope of this paper. That said, companies should research the physical location of the cloud provider's data center, as this could also have far-reaching legal effects on data privacy and portability. Awareness of and compliance with data protection regulations, such as HIPAA, usually remains the responsibility of the company, not the cloud provider. Furthermore, if the cloud provider is located offshore, ESI may be subject to the data protection laws of the country in which it is stored, thus affecting a company's ability to retrieve and control its own data.

[58] *Zubulake v. UBS Warburg*, 220 F.R.D. 212 (S.D.N.Y. 2003); *see also Pension Committee v. Banc of America Securities, LLC*, No. 05 Civ. 9016 (SAS), 2010 WL 184312, at *4 (S.D.N.Y. Jan. 15, 2010).

[59] Self-collection refers to the process of utilizing a company's own IT personnel, as opposed to a third party, such as an e-discovery vendor or forensic collection specialist, to copy and collect potentially relevant ESI.

[60] *Ward Gen. Ins. Serves., Inc. v. Employers Fire Ins. Co.*, 7 Cal. Rptr. 3d 844, 850-51 (Cal. App. 2003) ("We fail to see how *information, qua* information, can be said to have a material existence, be formed out of tangible matter, or be perceptible to the sense of touch. To be sure, information is stored in a physical medium, such as a magnetic disc or tape, or even as papers in three-ring binders or a file cabinet, but the information itself remains intangible. Here, the loss suffered by plaintiff was a loss of information, *i.e.*, the *sequence* of ones and zeroes stored by aligning small domains of magnetic material on the computer's hard drive in a machine readable manner. Plaintiff did not lose the tangible material of the storage medium. Rather, plaintiff lost the stored *information.* The sequence of ones and zeros can be altered, rearranged, or erased, without losing or damaging the tangible material of the storage medium."); *but see Hambrecht & Assocs., Inc. v. State Farm Lloyd's*, 119 S.W.3d 16 (Tex. App. Ct. 2003).

[61] *American Guar. & Liab. Ins. Co. v. Ingram Micro, Inc.*, NO. 99-185, 2000 WL 726789 (D. Ariz. Apr. 18, 2000).

[62] *Greco & Traficante v. Fidelity & Guar. Ins. Co.*, No. O52179, 2009 WL 162068, at *4-5 (Cal. App. Jan. 26, 2009) (concluding that mysterious loss of billing data, in absence of evidence that it had ever been "stored" on storage media, as required by the policy, and in the absence of damage to any computer equipment, was not direct physical loss to covered property).

[63] *See generally, Aspen Skiing Co. v. Aspen Highlands Skiing Corp.*, 472 U.S. 585, 602-03 (1985) (discussing market definition and power). A few types of inherently anticompetitive conduct, such as price fixing or agreements to divide markets, are treated as illegal "per se," meaning that they are illegal regardless of any showing of possession of market power in a relevant market by the participants. The conduct discussed in this paper, however, is unlikely to be viewed as illegal per se, and instead will be analyzed under the Rule of Reason, in which the competitive effects of the conduct on customers and participants in the relevant market are considered.

[64] The primary requirement for entry appears to be substantial available processing capacity. Phone companies, cable companies, universities and other such entities that typically have enormous computer processing capabilities all might be characterized, at least for now, as potential entrants into the market for provision of cloud services.

[65] See, e.g., Office Heads Into The Clouds: Microsoft Releases New Software Amid Cheap Online Alternative From Google, WALL ST. JOURNAL, May 13, 2010, at B7; The Digital Download Is Dead, SLATE MAGAZINE, May 21, 2010, http://www.slate.com/id/2254532/ (discussing theoretical competition between a future iTunes cloud and a Google/Android cloud music service).

[66] This analysis assumes that data storage and virus protection software are separate products for antitrust purposes (*i.e.* that consumers at least sometimes demand one without the other).

[67] The authors wish to acknowledge the efforts of Anthony Traymore in researching and helping to prepare this article. Anthony, a former associate of Reed Smith, now serves as in-house counsel at Sony Corporation.

[68] ISACA, Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives (2009).

[69] Id.

[70] Id.

[71] Id.

[72] Id.

[73] 15 U.S.C. § 6801-6809.

[74] 201 CME 17.00 (2009). The Massachusetts law requires, inter alia, encryption of NPPI, up-to-date firewall and malware solutions, and for a business to take reasonable steps to ensure that third-party service providers comply with the requirements.

[75] *See*, *e.g.*, Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness; Final Rule, 12 C.F.R. Part 30, et al. Requirements include exercising due diligence with service providers, requiring service providers by contract to implement appropriate measures, and monitoring service provider compliance. Appendix D, Section III (D).

[76] *See*, *e.g.*, FFIEC *Information Technology Examination Handbook* (2003–2010).

[77] *See*, The Payment Card Industry Data Security Standard, Version 1.2.1 (August 2009). Requirements include encryption of credit card account data when transmitted, and restriction of access to cardholder data to personnel on a "need-to-know" basis.

[78] SAFE Port Act, Pub.L. 109-347.

[79] FFIEC Guidance on Risk Management of Outsourced Technology Services, FIL 81-2000, 11/28/2000.

[80] No. 05-48, 7/05.

[81] Id.

[82] LogLogic, Inc. is a technology and application development company located in San Jose, California, that offers a comprehensive suite of log and security management products.

[83] Directive on privacy and electronic communications, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML (last visited June 10, 2010).

[84] The EU Directive grants the subjects of stored personal information certain rights, such as notice that their data is being collected and for what purposes, consent to any disclosure of their data, disclosure of who is collecting data, and access to and ability to correct their data. For additional discussion of these issues, *see* Robert Gellman, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, February 23, 2009, available at http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf (last visited June 14, 2011).

[85] Google Terms of Service, http://www.google.com/accounts/TOS (last visited June 13, 2011).

[86] EU Data Protection: Reforms Guide, http://www.eubusiness.com/topics/internet/data-protection.102 (last visited June 10, 2011).

[87] Newsweek.com Explores Amazon Cloud Computing, April 25, 2010, http://www.adweek.com/news/press/newsweekcom-explores-amazon-cloud-computing-115212

[88] Sun-Times Media Live with First Phase of DTI Cloud Conversion, October 28 2010, http://www.prweb.com/releases/2010/10/prweb4710144.htm (last visited, June 14, 2011)

[89] Amazon Elastic Cloud Compute, http://aws.amazon.com/ec2/.

[90] *See* Privacy Group Asks FTC to Investigate Google, March 18, 2009, http://www.pcworld.com/businesscenter/article/161497/privacy_group_asks_ftc_to_investigate_google.html.

[91] The authors would like to thank Jackie Penrod for her contributions and assistance with this article.

[92] Pub. L. 104-191.

[93] The Administrative Simplification Regulations were developed to, among other things: (i) establish standards for electronic health transactions (*e.g.*, claims, enrollment, eligibility, payment, coordination of benefits); (ii) address the security of electronic health information systems; and (iii) establish privacy standards for health information.

[94] 45 C.F.R. §§ 160, 162, 164.

[95] Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5 (Feb. 17, 2009). HITECH amended HIPAA with "improved privacy provisions and security provisions." Additionally, HITECH establishes incentive programs and other systems to encourage adoption and use of electronic and personal health records.

[96] 45 C.F.R. § 160.103.

[97] Id.

[98] Id.

[99] See id.

[100] *See* 75 Fed. Reg. 40,873 (July 14, 2010).

[101] *See* Law Librarian Blog: Privacy and Data Security Risks in Cloud Computing (Feb. 10, 2010) ("any HIPAA covered entity would first have to negotiate and enter into a business associate agreement with a cloud provider before it could store records in a cloud computing facility"), available at http://lawprofessors.typepad.com/law_librarian_blog/2010/02/privacy-and-data-security-risks-in-cloud-computing.html. This advice, however, presumes that all cloud services providers will be considered business associates.

[102] Multiple articles, blogs, and postings available on the Internet reveal uncertainty and debate among the various stakeholders and industry professionals as to whether cloud services providers act as business associates.

[103] 75 Fed. Reg. 40,872-40,873. (July 14, 2010). (Emphasis added).

[104] *Id.* As an example of a "downstream entity" relationship, the proposed rule states that if a business associate contracts with a company to handle document and media shredding to securely dispose of paper and electronic PHI, the subcontractor would be directly required to comply with the applicable requirements of the Security and Privacy Rules in conducting its work.

[105] 75 Fed. Reg. 40,873 (July 14, 2010).

[106] *See* 45 C.F.R. §§ 164.502(d); HITECH Act at Section 13401. De-identified health information is that which neither identifies nor provides a reasonable basis to identify an individual. 45 C.F.R. § 164.502(d)(2), 164.514(a), (b).

[107] Companies that provide personal health records are not necessarily covered entities or business associates. However, the provisions of HITECH apply certain elements of HIPAA to personal health record services providers. Section 13407, HITECH.

[108] Interoperability is also one of the requirements that an EHR services provider must demonstrate in order to become a certified provider. *See generally* www.healthit.hhs.gov (discussing certification of services provider programs).

[109] 45 C.F.R. §§ 164.105, 164.302-164.318. The Security Rule applies to "electronic protected health information that is created, received, maintained or transmitted by or on behalf of the health care component of the covered entity."

[110] A "workstation" is "an electronic computing device, for example, a laptop or desktop computer or any other device that performs similar functions, and electronic media stored in its immediate environment." 45 C.F.R. § 164.304.

[111] Under certain circumstances, PHI may be shared without first obtaining an authorization from the patient. *See* 45 C.F.R. § 164.512.

[112] HITECH defines "electronic health record" as "an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff."

[113] Section 13405(c)(1)(B), HITECH.