Navigating through the Cloud – Legal and Regulatory Management for Software as a Service

Jon M. Garon*

Contents

* Director, NKU Chase Law & Informatics Institute and Professor of Law, Northern Kentucky University Salmon P. Chase College of Law; J.D. Columbia University School of Law 1988. This paper was prepared on behalf of the 2012 NKY Security Symposium. A prior version was first presented at the 2011 Computer & Technology Law Institute. This working draft paper is available free of charge through SSRN at http://ssrn.com/abstract=2025246.

Introduction

Cloud computing has moved from a possible method of efficient data management to the industry standard for content management in many sectors. In response, new legal and regulatory standards for data privacy, security, and reliability are evolving to create a moving target for business, affecting all industries with data stored on remote servers.

Managing these challenges requires both vendors and customers to utilize comprehensive contracts and effective compliance efforts, particularly for international transactions and transactions involving health care, financial services or other regulated industries.

This review provides a roadmap to the practice of cloud computing and highlights the regulatory framework under which companies can take advantage of its efficiencies. It will also explore some of the contractual approach available to manage risk, achieve regulatory compliance, and better align the interests of the vendors and their customers.

What is Cloud Computing?

Last year was the breakout year for both the tablet and the cloud – and both trends are related.[1] "Cloud computing allows businesses and individuals to use the Internet to access software programs, applications, and data from computer data centers ….. Cloud computing services are not a unitary product but rather a continuum of services which businesses are able to access on an as-needed basis."[2] Among the services made available this year, Amazon, Google,

[1] *See, e.g.*, Lucas Mearian, *Apple iPad, other tablets seen driving SaaS, cloud storage Lack of internal storage will push users to online backup, synchronization services*, COMPUTERWORLD, Apr. 12, 2010, http://www.computerworld.com/s/article/9175148/Apple_iPad_other_tablets_seen_driving_SaaS_cloud_storage; Jamie Slattery, *What's the difference: iTunes Match vs Google Music Beta vs Amazon Cloud Player*, KNOW YOUR MOBILE, June 8, 2011, http://www.knowyourmobile.com/features/933178/whats_the_difference_itunes_match_vs_google_music_beta_vs_amazon_cloud_player.html.

[2] Int'l Bus. Machines Corp. v. Visentin, 31 I.E.R. Cas. (BNA) 1586 (S.D.N.Y. Feb. 16, 2011).

Apple and MP3.com have all created cloud music storage services.[3] While some of these music services are provided in arrangement with the record labels, MP3.com has successfully demonstrated that the cloud storage falls within statutory protections for online providers.[4]

In addition, services such as Dropbox, Box.net, Mozy, Spideroak, SugarSync, and Filesanywhere are a few of the services providing specialized document storage, but at the enterprise level, this field includes Google, AT&T, EMC, Amazon, IBM and other major providers. In some cases, these companies merely store files at a remote location; others synchronize the remotely stored data; while others provide software and full functionality from the remote locations to enable the user to have substantially unlimited access to both content and service.

In recent surveys, IT service provider CDW assessed the adoption of the cloud:

> CDW reported that 37 percent of health care companies maintain a written strategy for cloud computing, which puts them in the middle range of organizations that have taken this step. Of small businesses surveyed, 35 percent have a written strategy for cloud adoption, compared with 59 percent of large businesses, 41 percent of federal agencies, 29 percent of state and local governments, 29 percent of higher education institutions and 31 percent of K-12 schools.[5]

[3] David Kravets, *Judge OKs Unlicensed Cloud Music-Storage Service*, WIRED, (Aug. 22, 2011, 6:51 PM), http://www.wired.com/threatlevel/2011/08/mp3tunes-cloud-music-service/.

[4] *See* Capitol Records, Inc. v. MP3tunes, LLC, 2011 U.S. Dist. LEXIS 93351 (S.D.N.Y. Aug. 22, 2011) ("In the fall of 2005, MP3tunes added a storage service allowing users to store music files in personal online storage "lockers." Songs uploaded to a user's locker could be played and downloaded through any internet-enabled device. … MP3tunes' online storage system utilizes automatic and passive software to play back content stored at the direction of users. That is precisely the type of system routinely protected by the DMCA safe harbor." At the same time, however, MP3.com was liable for 350 songs for which EMI had provided a take-down notice but the notice was not followed).

[5] Brian T. Horowitz, *Health Care IT Industry Shies Away from Cloud Adoption: CDW*, EWEEK.COM, May 27, 2011, http://www.eweek.com/c/a/Health-Care-IT/Health-Care-IT-Industry-Shies-Away-From-Cloud-Adoption-CDW-293373/.

If cloud computing seems rather vague and ill-defined, that is because it is.[6] "[A]ll this vagueness and variation arise from the fact that the whole thing began in fancy and in dreaming; and that there are no rules of architecture for a castle in the clouds."[7] NIST has attempted to add some structural definitions upon which to begin placing the scaffolding of a common cloud nomenclature.[8] "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[9]

The cloud services all incorporate the essential characteristics of (i) on-demand, self-serve access; (ii) broad network access that agnostically accepts all devices – including computers, laptops, smart phones, game consoles and other network-enabled devises; (iii) resource pooling; (iv) rapid elasticity or scalability; and (v) measured service optimization so that "usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service."[10]

Despite the complex definitions, the legal issues for the cloud are only new in degree, not in type. Companies have been using third parties for data warehousing, communications, and remote applications for years in all industries including the data-critical areas such as health care

[6] *See, e.g.,* Mathias Thurman, *Security Manager's Journal: Giving cloud storage the ax*, COMPUTERWORLD, June 6, 2011, http://www.computerworld.com/s/article/356811/Cloud_Storage_Gets_the_Ax?taxonomyId=17.
[7] G.K. CHESTERTON, THE EVERLASTING MAN 64 (1925).
[8] Peter Mell & Timothy Grance, *The NIST Definition of Cloud Computing* 2 (Nat'l Inst. Stand. & Tech., NIST Special Publication 800-145 (Draft), Jan. 2011), *available at* http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf ("Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."). *See also*, Lee Badger, *et. al*, *Cloud Computing Synopsis and Recommendations*, (Nat'l Inst. Stand. & Tech., NIST Special Publication 800-146 2-1 (May 2012).
[9] Mell & Grace, *supra* note 8.
[10] *Id.*

and financial services.[11] The first iteration of this trend involved co-location agreements whereby the company's data remained housed on separately maintained servers.[12] Today, the information is comingled in massive, distributed server farms along with potentially petabytes[13] of data. NIST identifies four cloud deployment models:

> *Private cloud*. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
>
> *Community cloud*. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
>
> *Public cloud*. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
>
> *Hybrid cloud*. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).[14]

The private cloud essentially describes the existing vendor relationship between companies and their third party vendors. One of the leading data firms, Iron Mountain, stores "over 3 petabytes of PC data for some 3 million users in its secure offsite facilities worldwide."[15] Though it now describes its service as a cloud solution, Iron Mountain, like other secure data storage vendors, has been providing secure digital data storage since the mid-1990s in physically secure

[11] *E.g.*, 45 C.F.R. § 164.506(a) (2010) (limitations on health care data disclosure – "a covered entity may use or disclose protected health information for treatment, payment, or health care operations"); 16 C.F.R. pt. 316 (2006) (security safeguard rules regarding financial data).
[12] JACK W. PLUNKETT, PLUNKETT'S TELECOMMUNICATIONS INDUSTRY ALMANAC 2009 vi (Plunkett Research Ltd. 2008).
[13] Wikipedia.org, *Petabyte*, http://en.wikipedia.org/wiki/Petabyte (last visited Sept. 23, 2011) (A petabyte is equal in size to 1024 terabytes or one quadrillion bytes).
[14] Mell & Grance, *supra* note 8.
[15] Cloud Based Data Protection, http://www.ironmountain.com/resources/pcprotect/connected_security_brief.pdf (last visited Sept. 22, 2001).

facilities utilizing sophisticated data encryption and physical security to restrict access to data servers.[16]

Companies may be moving business applications to cloud services,[17] storing sensitive data with third-party vendors, or relying on business partners which are utilizing such services.[18]

> The core problem of cloud computing lies in guaranteeing *the integrity and confidentiality of the cloud user's data processing*, and this is true not only for personal data, but for any data that require confidentiality and integrity, such as business and trade secrets, research data, and any other data protected under intellectual property law. The goal is to prevent harmful, unauthorized access by third parties.[19]

The public cloud and hybrid cloud raise additional risks that business needs to manage. Unlike the direct one-to-one relationship between a business and private cloud vendor, a public cloud provider has a one-to-many relationship with every individual and entity using the cloud service. As a result, the contract is essentially a take-it-or-leave-it click-wrap agreement which may eviscerate legal protections for the customer of the cloud service.

Basic Cloud Security for the Consumer

At a minimum, cloud computing is really providing "software as a service" (SaaS), meaning "the consumer is to use the provider's applications running on a cloud infrastructure. The

---

[16] *Id.*

[17] Mell & Grance, *supra* note 8. Known as Cloud Software as a Service ("SaaS"), it is distinct from backup and storage services because all computing takes place on the vendor's equipment and significantly increases third party access to content.

[18] *See* American Institute of CPAs, Users and User Entities, http://www.aicpa.org/interestareas/accountingandauditing/resources/soc/pages/users.aspx.

> Many companies function more efficiently and profitably by outsourcing tasks or entire functions to service organizations that have the personnel, expertise, equipment, or technology to accomplish these tasks or functions. Examples of such services include cloud computing, managed security, health care claims management and processing, sales force automation etc. Although user management can delegate these tasks or functions to a service organization, they are usually held responsible by those charged with governance (for example, the board of directors), customers, shareholders, regulators and other affected parties for establishing effective controls over those outsourced functions.

Id.

[19] THILO WEICHERT, CLOUD COMPUTING & DATA PRIVACY, SEDONA CONF. WORKING GROUP SERIES 3, FEB. 2011 (translated into English by Lillian Clementi).

applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email)."[20] More robust models can also include the cloud platform or the cloud infrastructure as a service.[21]

Many consumer services are part of the public cloud. In addressing public cloud concerns, there are issues involving the contractual rights of the consumers as well as the ability of the consumer to address problems of data privacy and integrity. For example, the Sony Playstation network, Google Gmail system, and many other high-profile targets have been compromised.[22] Non-private clouds have more users and therefore more opportunities for vulnerabilities. They are also simply larger targets. Public cloud services may also fail to provide the level of data privacy and security necessary to protect the data or to assure the legal protections of confidentiality and trade secrets are met.

Private cloud configurations are not substantially different from the preexisting off-site service and storage relationships clients had with their vendors. But for non-private cloud computing, the key is scalability, which means that the infrastructure is built to accommodate large numbers of similarly situated customers who all have their data and services shared across applications and servers.

> Although not an essential characteristic of Cloud Computing in NIST's model, CSA has identified multi-tenancy as an important element of cloud. Multi-tenancy in cloud service models implies a need for policy-driven enforcement, segmentation, isolation, governance, service levels, and chargeback/billing models for different consumer constituencies. Consumers might utilize a public

[20] CLOUD SECURITY ALLIANCE, SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING 15-16 (Dec. 2009), https://cloudsecurityalliance.org/csaguide.pdf ("The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings." (quoting Mell & Grance, *supra* note 8, at 2)).
[21] *Id*. at 15-16.
[22] Hiawatha Bray, *Hackers and thieves a growing Web menace; Technology lag leaves systems vulnerable*, BOSTON GLOBE, June 11, 2011, at 1; *Hackers breach Citibank accounts 200K e-mail addresses, other information stolen*, STAR-LEDGER, June 10, 2011, at 19.

> cloud provider's service offerings or actually be from the same organization, such as different business units rather than distinct organizational entities, but would still share infrastructure.[23]

As a result of the multi-tenancy – or resource sharing – that occurs among the users of a cloud service, the individual customers have far less leverage or control in negotiating the data security and privacy provisions of the service agreement.

From the consumer's perspective, the risks associated with utilization of a cloud storage or SaaS provider can be analyzed through its terms-of-service-agreement/end-user-license-agreement and its operational steps to meet the obligations set forth in those consumer agreements.

Avoid Terms of Service that Give the Vendor Rights in Personal Data

Some services, such as Google's Gmail and Google Docs disclose in the terms of service that Google has access to the content of the documents.[24] The agreement is explicit in stating that Google has a non-exclusive license to exploit all the content provided by the users of these

[23] CLOUD SECURITY ALLIANCE, *supra* note 20, at 16.

[24] Google Terms of Service, http://www.google.com/accounts/TOS?hl=en (last visited Sept. 18, 2011).

> 11. Content license from you
>
> 11.1 You retain copyright and any other rights you already hold in Content which you submit, post or display on or through, the Services. By submitting, posting or displaying the content you give Google a perpetual, irrevocable, worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any Content which you submit, post or display on or through, the Services. This license is for the sole purpose of enabling Google to display, distribute and promote the Services and may be revoked for certain Services as defined in the Additional Terms of those Services.
>
> 11.2 You agree that this license includes a right for Google to make such Content available to other companies, organizations or individuals with whom Google has relationships for the provision of syndicated services, and to use such Content in connection with the provision of those services.
>
> 11.3 You understand that Google, in performing the required technical steps to provide the Services to our users, may (a) transmit or distribute your Content over various public networks and in various media; and (b) make such changes to your Content as are necessary to conform and adapt that Content to the technical requirements of connecting networks, devices, services or media. You agree that this license shall permit Google to take these actions.
>
> 11.4 You confirm and warrant to Google that you have all the rights, power and authority necessary to grant the above license.

Id.

services. As a legal matter, Google has fulfilled its duty, though it would not be a surprise to find that millions of users have not read these provisions and may not realize the disclosure being created.

A more interesting example comes from Dropbox. Used by 25 million people, Dropbox provides an effective combination of synchronizing computers and storing documents remotely.[25] Dropbox became notorious for allegedly overstating the security it provides for its customer.[26] Dropbox does not claim any right to a non-exclusive license of customer files or the rights to transfer information regarding the files to third parties.[27]At the same time, however, Dropbox has a rather broad exception allowing it to have use of its customers' files that goes beyond compliance with laws or court orders to include personal safety and to "prevent fraud or abuse of Dropbox or its users" and "Dropbox's property rights."[28] This also discloses that the

[25] I am a customer of Dropbox (using its free account). As I will discuss, however, I do not use it for either client information or student information covered by FERPA for the reasons discussed below.

[26] *See* G.F., *Internet security - Keys to the cloud castle*, THE ECONOMIST (May 18, 2011), http://www.economist.com/blogs/babbage/2011/05/internet_security.

[27] Dropbox Terms of Service, http://www.dropbox.com/terms (last visited Sept. 23, 2011).

> You retain full ownership to your stuff. We don't claim any ownership to any of it. These Terms do not grant us any rights to your stuff or intellectual property except for the limited rights that are needed to run the Services, as explained below.
>
> We may need your permission to do things you ask us to do with your stuff, for example, hosting your files, or sharing them at your direction. This includes product features visible to you, for example, image thumbnails or document previews. It also includes design choices we make to technically administer our Services, for example, how we redundantly backup data to keep it safe. You give us the permissions we need to do those things solely to provide the Services. This permission also extends to trusted third parties we work with to provide the Services, for example Amazon, which provides our storage space (again, only to provide the Services).
>
> To be clear, aside from the rare exceptions we identify in our Privacy Policy, no matter how the Services change, we won't share your content with others, including law enforcement, for any purpose unless you direct us to. How we collect and use your information generally is also explained in our Privacy Policy.

Id.

[28] Dropbox Privacy Policy, http://www.dropbox.com/terms#privacy (last visited Sept. 23, 2011).

> Compliance with Laws and Law Enforcement Requests; Protection of Dropbox's Rights. We may disclose to parties outside Dropbox files stored in your Dropbox and information about you that we collect when we have a good faith belief that disclosure is reasonably necessary to (a) comply with a law, regulation or compulsory legal request; (b) protect the safety of any person from death or serious bodily injury; (c) prevent fraud or abuse of Dropbox or its users; or (d) to protect Dropbox's property rights. If we provide your Dropbox files to a law enforcement agency as set forth above, we will remove Dropbox's encryption from the files before providing them to law

encryption utilized by Dropbox does not protect from Dropbox employees.[29] As a result of the public discussion of Dropbox's limitations and a FTC action brought by a cybersecurity expert, Dropbox has updated its terms and disclosure to make its policies more accurate.[30] Third party add-ons can also provide client-side encryption to further protect the data (which is a good idea anyway, if one carries sensitive data on a laptop or other device).[31] Spideroak, a direct competitor to Dropbox emphasizes its encryption system that places the encryption key on the user's computer – meaning that it cannot decrypt and disclose the files on its servers.[32] The security model, however, means that Spideroak is incapable of any password retrieval, so if the username or password is lost, or an executor of a decedent's estate needs access, the content is forever lost. Given the risk of permanent loss, many consumers may be making a very rational choice to risk the theoretical concern about Dropbox disclosure, and this may well suffice unless there is a legal obligation to treat the information more securely.

Consumers Should Adopt HTTPS and Secure Socket Layer Protections

Beyond storage and file synchronization, the consumer minimum can be found in the additional protection afforded by the encrypted "Hypertext Transfer Protocol Secure ("https") system. "Using an encryption algorithm, the "https:" tool gives users a mostly private channel to surf the web and share private information."[33]Any sensitive data, including online banking,

---

> enforcement. However, Dropbox will not be able to decrypt any files that you encrypted prior to storing them on Dropbox.

Id.

[29]*See* G.F., *supra* note 26.

[30] *See id*. (describing complaint by Chris Soghoian, filed May 11, 2011, http://www.wired.com/images_blogs/threatlevel/2011/05/dropbox-ftc-complaint-final.pdf).

[31] Simon Mackie, *SecretSync Adds Client-Side Encryption to Dropbox on the Fly*, WEBWORKERDAILY, (May 17, 2011), http://gigaom.com/collaboration/secretsync-adds-client-side-encryption-to-dropbox-on-the-fly/.

[32] Spideroak, https://spideroak.com/ (last visited Sept. 23, 2001). *See also* G.F., *supra* note 26 (discussing the differences in approach).

[33] *Security in 60 Seconds - How to Fight Back Against Hackers and Protect Yourself on the Web*, VOICE OF AMERICA, (Aug. 22, 2011), http://blogs.voanews.com/digital-frontiers/2011/08/22/security-in-60-seconds/.

healthcare or other information a person considers sensitive should be sent only using this protocol. More and more vendors are utilizing the https as their default standard.

At the same time, however, nothing is wholly secure. A Farsi-speaking hacker recently breached a Dutch certificate authority, DigiNotar, and used DigiNotar's legitimate certifying authority to issue false SSL Certificates – the tools used to assure that your data is traveling to the entity one believes is on the other side of the transaction.[34] With false Secure Socket Layer ("SSL") certificates, the hackers could intercept data mid-transfer to monitor or re-use that information. This is evidently the first breach of the SSL certificates and Microsoft, Apple and the browser providers have moved quickly to block the DigiNotar certificates. But it serves as a reminder that all security is based on industry precautions, best efforts and ongoing vigilance. No system will be impenetrable. A good system will be responsive to threats and be continually updated; it cannot promise absolute security.

Basic Cloud Security for the Business Customer

For a corporate account, minimum precautions are required, regardless of the industry. Interestingly, NIST have provided some basis in its technical overview.[35] These arrangements are typically bifurcated, with a service agreement providing for the economic terms of the agreement and a service level agreement "stating the technical performance promises made by a provider including remedies for performance failures."[36]

The service level agreements typically emphasize for key concepts: uptime service availability and service credit for failure to meet these service availability obligations; data preservation policies; and compliance with the customer's legal obligations to meet data privacy

[34] Steven J. Vaughan-Nichols, *Fake SSL certificates pirate Web sites*, ZD NET (Sept. 6, 2011, 3:21 PM), http://www.zdnet.com/blog/networking/fake-ssl-certificates-pirate-web-sites/1428.
[35] Badger, *supra* note 9 at 3-1.
[36] *Id*.

and security obligations.[37] For the legal team, this list should be a bit longer. "The main legal concerns related to the cloud model are related to data protection and data security; confidentiality of the information and intellectual property; law enforcement access; cloud service providers (CSPs) professional negligence; subcontracting of cloud services and CSP change of control; and 'vendor lock in'."[38] "Besides service level guarantees and remedies, a good SLA will contain service definitions, disaster recovery provisions, customer duties and software management and upgrade practices."[39]

Service interruption can be handled through the service level agreement but companies may need to address some of its service level risk by understanding the vendor's risk management solutions as well as understanding the redundancy built into the vendors' processes. Operational credits will do a company little good if it opens the business to reputational loss or liability to its own clients.[40]

What is often treated as boilerplate becomes critical in this regard. The remedy for uptime failure is typically in the form of service credit. But service credit is unhelpful and insufficient for data breaches that would result in mandatory consumer breach notification obligations, professional negligence, subcontracting, or acts which results in corporate liability under various laws or regulations.[41]

---

[37] *Id*. at 3-1-2.
[38] Paolo Balboni, *Cloud Computing main legal concerns*, ADVANCED THREAT REPORT, June 10, 2010 at http://www.infosecurity-magazine.com/blog/2010/10/6/cloud-computing-main-legal-concerns/227.aspx (last visited Oct. 7, 2012).
[39] *See* Robert J. Scott, *Taking the Risk Out of Cloud Computing*, EVERYTHING BUS. CORP!, Sept. 16, 2010 at http://www.corpmagazine.com/technology/digital/itemid/1805/taking-the-risk-out-of-cloud-computing (last visited Oct. 7, 2012) .
[40] *Id.*
[41] See *User Guide: Cloud Computing Contracts, SLAs and Terms & Conditions of Use*, JISCLEGAL, Aug. 31, 2011, at http://www.jisclegal.ac.uk/ManageContent/ViewDetail/ID/2141/User-Guide-Cloud-Computing-Contracts-SLAs-and-Terms-Conditions-of-Use-31082011.aspx (last visited Oct. 7, 2012).

Consumer Cloud Products are not intended for Business Use

Business customers should not use consumer services. For example, relying on the terms of service of Google could be a substantial problem. Even companies operating in unregulated industries must comply with their own stated privacy and security policies.[42] Unless those policies state that the company shares all data with the world, or the policy specifically includes Google's non-exclusive license, the use of these consumer tools for business could (and should) give rise to liability.[43] The vast majority of jurisdictions also have data security breach notification laws, so a poorly selected vendor can open a company to embarrassment and even liability if its vendor is itself out of compliance in the event of a breach.[44]

A second concern for the general business is the ownership of content, with widely adopted services like the public services of Google transferring a non-exclusive copyright license to the advertising and search giant.[45] Facebook also extracts such a non-exclusive license.[46] These

[42] *Section 5 of the FTC Act*, IT LAW WIKI, http://itlaw.wikia.com/wiki/Section_5_of_the_FTC_Act (last visited Sept. 18, 2011) ("The FTC has taken action against websites for violating their own privacy policies as a deceptive trade practice."); Customer Information And Privacy, Safeselling.org, http://www.safeselling.org/privacy.shtml#2 (last visited Sept. 25, 2011) ("Using its authority under Section 5 of the FTC Act, which prohibits unfair or deceptive practices, the Commission enforces the promises in privacy statements, including promises about the security of consumers' personal information.").

[43] Google uses a different license for its corporate and educational clients. *See*, *e.g.*, Google Apps for Business Online Agreement, http://www.google.com/apps/intl/en/terms/premier_terms.html (last visited Sept. 23, 2011) ("7.1 Intellectual Property Rights. Except as expressly set forth herein, this Agreement does not grant either party any rights, implied or otherwise, to the other's content or any of the other's intellectual property. As between the parties, Customer owns all Intellectual Property Rights in Customer Data, and Google owns all Intellectual Property Rights in the Services.").

[44] *See* Nat. Conf. of State Legislatures, State Security Breach Notification Laws, http://www.ncsl.org/default.aspx?tabid=13489 (last visited Sept. 23, 2011) ("Forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information.").

[45] *E.g.*, Google Terms of Service, http://www.google.com/apps/intl/en/terms/user_terms.html (last visited Sept.23, 2011). *See* Jon M. Garon, *Searching Inside Google: Cases, Controversies and the Future of the World's Most Provocative Company*, 30 LOYOLA OF L.A. L. REV. 429 (2010). In contrast, Google's terms of service for its business services and academic services establish much higher privacy and security requirements, including a recognition by Google that it is governed by FERPA regarding for academic customers. *See* Google Apps for Education Agreement, http://www.google.com/apps/intl/en/terms/education_terms.html (last visited Sept. 23, 2011).

[46] Facebook, Statement of Rights and Responsibilities, https://www.facebook.com/terms.php (last visited Sept. 23, 2011) ("For content that is covered by intellectual property rights, like photos and videos ("IP content"), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-

licenses may not be consistent with the licenses under which a company acquired rights to stock photographs, artwork or other intellectual property it exploits.

Use of social media may be essential for business marketing and customer relations, but the content posted on those sites should be carefully cleared to be sure the company has the rights to distribute in that media. Similarly, the enforcement of intellectual property rights in social media is often challenging, so companies should think carefully regarding the value of the assets they distribute. Companies need to balance the value of the social media interaction with the value of the copyrighted work to assess the risks of rampant public copying. If the unauthorized redistribution does only modest harm (or serves as viral marketing), then there is little risk; if the work would otherwise sell for a very high value in other distribution channels, then trying to maintain control of that work on social media may not make strategic sense.

Audit Requirements under SSAE 16 (SOC 2 and SOC 3)

Beyond the use of consumer tools to operate a business, small enterprises must view their duty regarding customer data in the same fashion as do Fortune 500 companies. For many vendors this is a daunting task. As of June 15, 2011 new standards create more comprehensive reporting requirements.[47]

Prior to June 2011, to assure minimum standards were being met by such services, the SAS 70 report was used to verify "that the controls and processes that the data center operator has in place are followed."[48] The SAS 70 report, however, may have created a false sense of security

exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook").

[47] *The SSAE16 Auditing Standard*, SSAE-16.COM, Aug. 23rd, 2012 at http://www.ssae-16.com/ (last visited Oct. 7, 2012).

[48] Cloud Based Data Protection, *supra* note 15.

because it did not set minimum standards or establish best practices.[49] It merely focused on compliance with a company's reported systems rather than any minimum standard setting. In the past year, however, this system has been updated. Auditors have been demanding greater accountability, and fortunately the vendors are responding.[50]

The American Institute of CPAs (AICPA) has replaced the SAS70 with the SSAE 16, effective June 15, 2011.[51] Under SSAE 16, SOC 2 and SOC 3 reports "provide much more stringent audit requirements with a stronger set of controls and requirements specifically designed around data center service organizations.[52] These audit reports create the new baseline for vendor contracting. "SSAE 16 goes beyond SAS 70 by requiring the auditor to obtain a written assertion from management regarding the design and operating effectiveness of the controls being reviewed."[53]

The AICPA standards focus on five key areas of review:

These five key system attributes are described by AICPA:

- *Security*: The system is protected against unauthorized access (both physical and logistical).

[49] Mike Klein, *SAS 70, SSAE 16, SOC 2 and SOC 3 Data Center Standards*, ONLINE TECH – OTBLOG (Feb. 15, 2011), http://resource.onlinetech.com/sas-70-ssae-16-soc-2-and-soc-3-data-center-standards/. ("There is no minimum bar that the data center operator has to achieve and no benchmark to hold data center operators accountable to. A data center with strong controls and processes can claim the same level of audit as a data center operator with weak controls and systems. The only way a user can tell the difference is to read through the detailed audit report.").

[50] *Id.*

[51] AICPA has certified auditing practices that create reliable assurance of data reliability and risk management. American Institute of CPSs, Welcome to the AICPA, http://www.aicpa.org (last visited Sept. 23, 2011).

AICPA has recently replaced the SAS70 with the "Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization." (SSAE 16) *See* http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/faqs_service_orgs.pdf.

[52] *Id*. Under SSAE 16, SOC 2 and SOC 3 reports "provide much more stringent audit requirements with a stronger set of controls and requirements specifically designed around data center service organizations. SOC 2 and SOC 3 provide a standard benchmark by which two data center audits can be compared against the same set of criteria. In contrast to an SSAE-16 engagement, where the data center operator defines the criteria for an audit, the SOC 2 Report uses specifically pre-defined control criteria related to 1) security, 2) availability, 3) processing integrity, 4) confidentiality or 5) privacy of a system and its information." Klein, *supra* note 41.

[53] Klein,*supra* note 41.

- *Availability*: The system is available for operation and use as committed or agreed.
- *Processing integrity*: System processing is complete, accurate, timely and authorized.
- *Confidentiality*: Information designated as confidential is protected as committed or agreed.
- *Privacy*: Personal information is collected, used, retained, disclosed and disposed of in conformity with the commitments in the entity's privacy notice, and with criteria set forth in *Generally Accepted Privacy Principles*.[54]

These five attributes of an information system cover the key attributes for a properly operating security and privacy regime. It includes the privacy policy adopted by the company – as informed by the AICPA's reasonably stringent best practices regarding privacy, additional confidentiality provisions of the service, the physical as well as technical aspects of data protection, and the operational reliability. Today's coverage by the AICPA is a significant improvement of that previously provided.

Despite these additions, however, there are important limitations that must be taken into account. To rely on the SSAE 16, a customer of a cloud service must understand the nature of the report being sought. Companies that claim SSAE 16 compliance need to do more than order a report because the Type 1 report is an internal report not appropriate for use by potential customers.[55] Moreover, the Type 1 report probably remains inadequate for most companies, because it does not set the standards for data security and other protections, but instead merely assesses the compliance of the vendor's efforts to meet the standards that vendor selected. If the vendor selected minimal standards, then the report will only reflect that those minimum standards were or were not met.

---

[54]AICPA. *See also* Thomas Shaw, *Changes Continue for Cloud Service Provider Controls*, LAW TECH. NEWS, June 22, 2011, http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202498009028.

[55] *See* UHY LLP, SOCS AND SASS: THE NEW STANDARDS FOR SERVICE ORGANIZATION CONTROLS REPORTING 1 (2011), http://www.uhyadvisors-us.com/uhy/LinkClick.aspx?fileticket=BA2FRCgY4JI=.

A Type 2 report provides substantially greater assurance. "A Type 2 SOC 1 report provides the auditors' opinion as to the accuracy and completeness, the suitability of the design of controls, AND the operating effectiveness of the controls throughout a declared time period, generally between six months and one year."[56] While there is always room for interpretation and variations among auditors, the Type 2 report has considerably more assessment value than the Type 1 report.

A blog post by Reliable Networks provides some interesting insight into the application of the business decision involving audit compliance:

> At the risk of over-simplifying, a SOC 1 is at its core a *financial* audit whereas a SOC 2 is an *operational* audit. For a SOC 2 Type II, you have to plan your work, work your plan, and document everything from soup to nuts along the way, with a very clear operational audit trail. …
>
> In deciding to pursue a SOC 2 over a SOC 1, we interviewed a number of prospective clients in regulated industries (mostly outside of Maine, in New York City, Chicago and California) which represent our target market of clients running mission-critical systems with sensitive/regulated/proprietary data. The majority told us that during 2012 and 2013, they would be requiring their existing vendors to obtain a SOC 2 Type II and that starting in 2013 only vendors with a SOC 2 Type II would be eligible for work; a SOC 1 was simply "not good enough".
>
> To be fair, a SOC 1, mis-used or not, is "good enough" for a number of companies, but our typical client requires us to adhere to a higher set of standards.[57]

A variation of the Type 2 report can be disclosed as a Type 3 report, which basically strips certain internal reporting information from the Type 2 report so that the report can be made

[56] *Id.*
[57] *Reliable Networks On The Move! SSAE 16 SOC 2 Type II Ongoing*…, RELIABLE NETWORKS, http://www.reliablenetworks.com/security/reliable-networks-move-ssae-16-soc-2-type-ii-ongoing/ (last visited Oct. 7, 2012).

available to potential customers and the general public.[58] The Type 3 report includes a certification or seal of approval that can be used by the reporting company to show its compliance with the SSAE 16 standards.

It remains unclear how widely adopted the SOC 3 certification will become. Contractually, companies such as Google use terms like "reasonable" to adjust their practices with the rapidly evolving security norms.[59] Their contract provisions include the following:

> 1.1 **Facilities and Data Transfer**. All facilities used to store and process Customer Data will adhere to reasonable security standards no less protective than the security standards at facilities where Google stores and processes its own information of a similar type. Google has implemented at least industry standard systems and procedures to ensure the security and confidentiality of Customer Data, protect against anticipated threats or hazards to the security or integrity of Customer Data, and protect against unauthorized access to or use of Customer Data. As part of providing the Services, Google may transfer, store and process Customer Data in the United States or any other country in which Google or its agents maintain facilities. By using the Services, Customer consents to this transfer, processing and storage of Customer Data.[60]

As described by Google, it meets "reasonable security standards" and those standards are the same Google uses for its own, similar data. As a practical matter, this creates a strong incentive for Google to be constantly improving the data security for its customers because it has strong business incentives to protect its own data. For general merchants, it has yet to be a heavily scrutinized question, (though as discussed below, there is much greater statutory guidance and case-law in the areas of financial services).

---

[58] *Id*. at 2 ("The SOC 3 report does not contain any details about the service auditor's testing or the results of the testing. A SOC 3 report is a general use report, available to existing and potential customers as well as the general public.").

[59] *See, e.g*. Claridge v. RockYou, Inc., 2011 U.S. Dist. LEXIS 39145, 17-18 (N.D. Cal. Apr. 11, 2011) (court dismissed claim under Cal. Penal Code § 502(c)(6) (2011) that the failure to provide reasonable security can be actionable as "[k]nowingly and without permission provid[ing] or assist[ing] in providing a means of accessing a computer, computer system …").

[60] Google Apps for Business Online Agreement, *supra* note 36.

One aspect of these standards applies to trade secrets. There is a critical concern on public clouds regarding the ability to protect confidential business information, typically protected through trade secret law. "The subject of a trade secret must be secret, and must not be of public knowledge or of a general knowledge in the trade or business."[61] "This necessary element of secrecy is not lost, however, if the holder of the trade secret reveals the trade secret to another "in confidence, and under an implied obligation not to use or disclose it.""[62] In addition to the necessary restrictions on disclosure, trade secret laws such as the Uniform Trade Secrets Act require that a trade secret be "the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[63] So at a minimum any use of cloud computer services must include an obligation by the cloud service provider not to access, use or disclose any trade secrets (other than for the legitimate purposes of maintaining the service).[64] Without such an obligation, the trade secret is disclosed and the confidence breached.[65]

[61] Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974).
[62] *Id*. (quoting Cincinnati Bell Foundry Co. v. Dodds, 10 Ohio Dec. Reprint 154, 156, 19 Weekly L. Bull. 84 (Super.Ct. 1887)).
[63] UNIF.TRADE SECRETS ACT, 1(4) (1985).

> "Trade secret" means information, including formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Id.
[64] *See, e.g.*, Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 923 F. Supp. 1231, 1253 (N.D. Cal. 1995) ("'Reasonable efforts' can include advising employees of the existence of a trade secret, limiting access to the information on a 'need to know basis,' requiring employees to sign confidentiality agreements, and keeping secret documents under lock.") (internal citations omitted).
[65] Google provides such a provision, albeit in a very generalized manner:

> 6.1 Obligations. Each party will: (a) protect the other party's Confidential Information with the same standard of care it uses to protect its own Confidential Information; and (b) not disclose the Confidential Information, except to Affiliates, employees and agents who need to know it and who have agreed in writing to keep it confidential. Each party (and any Affiliates, employees and agents to whom it has disclosed Confidential Information) may use Confidential Information only to exercise rights and fulfill its obligations under this Agreement, while using reasonable care to protect it. Each party is responsible for any actions of its Affiliates, employees and agents in violation of this Section.

Beyond this naked obligation, what remains to be determined is the level of data protection required by the cloud computing service to meet the requirement that the steps to protect a trade secret are reasonable under the circumstances.[66] There do not yet seem to be cases related to the exploitation of trade secrets by third parties stolen from cloud computing services. Perhaps this means the concern is overstated or perhaps this suggests the proof that trade secret data was acquired through cloud espionage is difficult to establish. In addition, since most trade secret cases seem to involve former employees acting against the interest of their previous employer, there is an additional risk that the ease of posting content to public venues raises the specter that outgoing employees will disclose information in a manner that destroys the trade secret so that they can take advantage of the information in their new positions.

Credit Card Security – PCI Compliance

For merchants using credit cards, a more powerful regulator has emerged – their credit card vendor. Five major credit card companies (Visa, MasterCard, American Express, Discover, and JCB[67]) combined in 2006 to establish the PCI Security Standards Council and create a set of uniform data compliance procedures.[68] As Bob Russo, the PCI Council general manager explains,

> PCI, which stands for Payment Card Industry, [sets a] data security standard. It's a set of 12 specific requirements that cover six different goals. It's very prescriptive. It says not only that you need to be secure but it tells you how to become secure. It's more about security than compliance. The goals are things like

Google Apps for Business Online Agreement, *supra* note 36. The capitalized term is never defined under the agreement. This article draws no conclusion regarding the validity, enforceability or unenforceability of this provision.

[66] *See* Gates Rubber Co. v. Bando Chemical Indus., Ltd., 9 F.3d 823, 849 (10th Cir. 1993) (limited disclosures may not destroy a trade secret); Rockwell Graphic Sys., Inc. v. DEV Industries, Inc., 925 F.2d 174 (7th Cir. 1991) (disclosure can be made to company vendors).

[67] Japanese Credit Bureau.

[68] *See* Elinor Mills, *PCI compliance: What it is and why it matters (Q&A)*, CNET NEWS, Feb. 8, 2010, http://news.cnet.com/8301-27080_3-10448197-245.html (interview with Bob Russo, general manager of the PCI Security Standards Council).

> build and maintain a secure network, protect card holder data and regularly monitor and test the networks. That's the main standard.
>
> We manage three different standards. The first one covers everything from the physical security to logical security. The second standard is PADSS, Payment Application Data Security Standard. These are for payment applications a merchant would buy off the shelf. … We make sure these applications aren't storing prohibitive data, such as data on the magnetic strip on the card. …
>
> The last piece we manage is called PTS, PIN Transaction System. Anytime you enter a PIN number, for example, this standard would take effect. It looks at those PIN entry devices so when you go to a large department store and you buy something and you use a debit card they'll hand you a PIN pad and you key in your number. We certify those devices as well as unattended payment terminals, such as those used at gas station [islands], ticket kiosks, and transit systems, like the Boston underground.[69]

The twelve steps involved in PCI compliance are rather straight-forward:

Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored data 4. Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security[70]

These twelve steps provide very straight-forward advice to any vendor with access to data. While the specifics can become a challenge for some companies, the notions of using strong passwords, restricting physical access to data, not storing credit card information once

[69] *Id.*
[70] Visa Cardholder Information Security Program, http://usa.visa.com/merchants/risk_management/cisp_overview.html (last visited Sept. 18, 2011).

authorization has occurred, maintaining information security policies, updating antivirus and other patches, and testing security all make common sense.

The most important aspect of PCI compliance is that it is a moving target. Hackers and identity thieves exploit newly discovered vulnerabilities and companies that fail to update the firewalls, antivirus software and equipment hardware become the most vulnerable. PCI general manager Russo claims that none of the major credit card breaches involved compliant systems, though some of the systems had originally been compliant but failed to maintain their updates.[71]

In coming years, the PCI standard will evolve. Visa, for example, has announced that it will substantially accelerate the use of near field communication chips (like RFID tags) that utilize both the card data and chip-to-chip communications that make it much more difficult to create fraudulent cards.[72]

Cloud Computing Security for Financial Services Providers

Companies involved in financial services[73] transactions have a number of additional obligations regarding customer information under the Gramm-Leach-Bliley Act of 1998.[74] Focusing on cloud computing issues, regulators have created the FTC Safeguards Rule that outlines the steps needed to protect customer information.[75]

[71] Mills, *supra* note 59.
[72] *Visa Announces Plans to Accelerate Chip Migration and Adoption of Mobile Payments*, Visa Press Release, Aug. 9, 2011, *available at* http://corporate.visa.com/media-center/press-releases/press1142.jsp.
[73] *See* 16 C.F.R. 313.3(k)(2) (2003); R. Bradley McMahon, *Note: After Billions Spent to Comply With HIPAA And GLBA Privacy Provisions, Why is Identity Theft the Most Prevalent Crime in America?*, 49 VILL. L. REV. 625, 634-635 (2004) ("Financial institutions under the Act include everything from real estate appraisers to automobile dealerships.").
[74] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, Title V, §§ 501-527, 113 Stat. 1338 (1999) (financial services).
[75] *See, e.g.* FTC Safeguards Rule, 16 C.F.R. pt. 314 (2010) (implementing GLB Act §§ 501(b), 505(b)(2), 15 U.S.C. §§ 6801(b), 6805(b)(2)).

Among the steps required, the Safeguard Rule -

> The Safeguards Rule requires companies to develop a written information security plan that describes their program to protect customer information. The plan must be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each company must:
>
> - designate one or more employees to coordinate its information security program;
> - identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
> - design and implement a safeguards program, and regularly monitor and test it;
> - select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information; and
> - evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.[76]

These requirements provide a comprehensive set of obligations to manage employee selection, supervision and training, physical security of data, encryption and authentication protocols, and notification steps. These requirement have no specific prohibition or endorsement of cloud computing or SaaS protocols. Instead, the adoption of any SaaS or other service must meet the same standards as the typical third-party agreement with outside vendors.

> A number of courts have recognized that fiduciary institutions have a common law duty to protect their members' or customers' confidential information against identity theft.[77] … If this duty not to disclose customer information is to have any weight in the age of online banking, then banks must certainly employ sufficient security measures to protect their customers' online accounts.[78]

---

[76] *FTC Facts for Business, Financial Institutions and Customer Information: Complying with the Safeguards Rule*, FTC (Apr. 2006), http://business.ftc.gov/documents/bus54-financial-institutions-and-customer-information-complying-safeguards-rule.pdf.

[77] Shames-Yeakel v. Citizens Fin. Bank, 677 F. Supp. 2d 994, 1008-1009 (N.D. Ill. 2009) *citing* Jones v. Commerce Bancorp, Inc., No. 06 Civ. 835, 2006 U.S. Dist. LEXIS 32067, 2006 WL 1409492, at *2 (S.D.N.Y. May 23, 2006); Bell v. Mich. Council 25 of Am. Federation of State, County, Municipal Employees, No. 246684, 2005 Mich. App. LEXIS 353, 2005 WL 356306, at *1 (Mich. Ct. App. Feb. 15, 2005) (per curiam).

[78] *Id.*

Under both the common law standards and the GLB Act standards, there is a duty to protect the customer from identity theft, which includes a duty not to expose the protected information to theft from employees. In the case of cloud computing, one particular concern regarding this standard is the inability to actually monitor or police the server farms on which data is stored or the training and supervision of the employees involved in this process.[79]

This duty may be met in two ways. First, the SaaS vendor could agree to a negotiated set of steps that it will take and monitor to assure that its own staffing, physical and technical protection measures meet or exceed that of the financial service institutions as well as agree to monitoring by the financial service institution of the standards. Perhaps the SOC 2 and SOC 3 certification will eventually come to be recognized as sufficient in this regard and independent auditors can perform this function.

Alternatively, comprehensive robust end-to-end encryption may suffice to allow the financial institution to essentially disregard the employee and physical safeguard concerns on the reasonable basis that the cloud vendor cannot access the data in its decrypted form and therefore theft and misuse are reduced to rather minor concerns. This approach does not address the increasingly common situation in which a bank is utilizing a third party service provider as its online banking provider or otherwise allowing the vendor direct access to its customers. In those situations, the vendor necessarily has direct access to the protected customer information and must itself operate within the guidelines of the FTC Safeguards Rule.

One simple way to provide for this by contract is to include the reference directly. Contracts for third party vendors providing data security and privacy services can incorporate the essential

[79] WAYNE JANSEN & TIMOTHY GRANCE, GUIDELINES ON SECURITY AND PRIVACY IN PUBLIC CLOUD COMPUTING, NIST DRAFT SPECIAL PUBLICATION 800-144, 16 (Jan. 2011) ("Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and, in doing so, confers an unprecedented level of trust onto the cloud provider.").

statutory obligations for service by incorporating the legal standards into the duties under the contract. In the financial sector, for example, duties regarding data privacy, security and integrity can be subject to a "commercially reasonable" standard as provided:

> "Commercially Reasonable" means the steps necessary to protect the data privacy and security of a charted financial institution, including without limitation, compliance with applicable data privacy and security obligations pursuant to the GLB Act, 15 U.S.C. §§ 6801- 6827 (2011) and accompanying regulations as may be amended from time to time; by the Federal Financial Institutions Examination Council's (FFIEC); and applicable state and federal data breach notifications statutes and regulations.

Like the paragraph above, the successful cloud service agreement will establish the contractual and legal duties of the vendor, along with tools for the business to assure compliance.[80] Key provisions in a private cloud vendor agreement include:

- The duty to meet applicable regulatory guidelines as a covered entity or third party recipient of data.
- The duty to utilize best practices to assure data privacy, security and integrity.
- The duty to report any data security breach and meet applicable state and federal notification obligations.
- The obligations to physically secure the information, by controlling physical access to computers, servers and equipment.
- The duty and practices to manage vendor personnel in a manner that restricts access to stored information from non-essential personnel, to train its personnel to meet data privacy and security practices, and to immediately cut-off access to former employees.
- Meaningful indemnification provisions and the financial ability to meet such obligations.
- Restrictions on exploitation of aggregate data analysis and metadata analysis.[81]

Other issues to be addressed include the international movement of data and any additional obligations triggered by out-of-county transactions; the data retention policies of the vendor to avoid excessively long retention of documents and data thought destroyed by the business; data

[80] Tanya Forsheit, *Contracting for Cloud Computing Services: Privacy and Data Security Considerations*, PRIVACY & SECURITY LAW REPORT, 9PVLR20, May 17, 2010, at 1-2.

[81] The aggregation of services by large vendors creates opportunities to track and study the data flow. Even if done on an aggregate basis, however, the use of health care or customer financial data may not be authorized and should be contractually restricted.

formatting, translating and migrating concerns; and insurance coverage regarding loss of data residing exclusively in the cloud.[82]

Cloud Computing Security for Health Care Providers

The category of data most heavily regulated in the U.S. falls within the category of personal health care data protected by HIPAA and the HITECH Act.[83] The accompanying regulations provide comprehensive data security provisions to protect patient privacy and to reduce medical fraud. "Although identity theft is usually associated with financial transactions, it also happens in the context of medical care. According to [FTC] medical identity theft occurs when someone uses another person's name or insurance information to get medical treatment, prescription drugs or surgery. It also happens when dishonest people working in a medical setting use another person's information to submit false bills to insurance companies."[84]

Guidance regarding the HIPAA security rules is provided by the Office for Civil Rights.[85] The security rules cover, *inter alia*, all electronic personal health information ("e-PHI"). The risk analysis which must be conducted regularly, while similar to the risk analysis undertaken by financial institutions, is that much more rigorous.[86]

---

[82] James Bourke, *Doing Business in the Cloud*, TECHBYTE CPA INSIDER (Aug. 23, 2010) http://www.cpa2biz.com/Content/media/PRODUCER_CONTENT/Newsletters/Articles_2010/CPA/Aug/DoingBusinessInCloud.jsp.

[83] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified at 29 U.S.C. §§ 1181-1182 (Supp. III 1997)); Health Information Technology for Economic and Clinical Health Act of 2009, Pub. L. No. 111-5, 123 Stat. 226 (codified at 42 U.S.C. § 17932). S*ee also* U.S. Dep't of Health & Human Servs., Standards for Electronic Transaction, Final Rule 65 Fed. Reg. 50312-72 (codified at 45 C.F.R. Pts. 160 & 162 (privacy regulations adopted by the Secretary of Health and Human Services)).

[84] Medical Identity Theft: FAQs for Health Care Providers and Health Plans, Bureau of Consumer Protection http://business.ftc.gov/documents/bus75-medical-identity-theft-faq-health-care-health-plan (last visited Sept. 18, 2011).

[85] 45 C.F.R. §§ 164.302 – 318.

[86] *See* Michael F. Schaff & Glenn P. Prives, *Under HITECH, What are Your Client's Obligations When There is a Breach of Patient Records?*, WILENTZ GOLDMAN & SPITZER PA, http://www.wilentz.com/Files/ArticlesandPublicationsFileFiles/212/ArticlePublicationFile/Schaff%20Prives%20AHLA.pdf (last visited Sept. 18, 2011).

The good news is that NIST suggests "[m]any cloud providers meet standards for operational compliance and certification in areas like healthcare …."[87] "HIPAA requires both technical and physical safeguards for controlling access to data, which may create compliance issues for some cloud providers."[88] Still, despite the recognition, there are many challenges. "Data stored in the cloud typically resides in a shared environment collocated with data from other customers. Organizations moving sensitive and regulated data into the cloud, therefore, must account for the means by which access to the data is controlled and the data is kept secure."[89] The methods discussed above for encryption and entity-level compliance are available to health care providers looking for cloud solutions as well as financial organizations. But the requirements for compliance are more stringent.

While it may also be a matter of degree, the importance of data integrity and availability may be more acute with e-PHI than with financial data or other protected data.[90]

Still, there is a different dynamic at play for health care organizations – the duty to their patients. Under HHS guidelines, "80 percent of patients [should be able] to access their [electronic health records (EHRs)] within 36 hours of discharge from the facility. In addition, at least 20 percent of patients must be allowed access to EHRs, including test results."[91] This effort is not moving quickly. "The patient could be considered "forgotten" as a user of EHRs, according to Bruce Henderson, director and national leader of PwC's EHR-HIE practice. … Physicians believed 45 days was a reasonable amount of time to make test results available

[87] JANSEN & GRANCE, *supra* note 70 at 8.
[88] *Id*. at 16. The NIST Guidance recognizes the similarities with PCI and GLBA obligations as well.
[89] *Id*. at 24.
[90] *See, e.g.*, Dan Goodin, *Salesforce.com Outage Exposes Cloud's Dark Linings*, THE REGISTER (Jan. 6, 2009), http://www.theregister.co.uk/2009/01/06/salesforce_outage/.
[91] Brian Horowitz, *Hospitals Must Seek Patient Input on EHRs to Achieve 'Meaningful Use': PwC*, EWEEK.COM, Mar. 7, 2011, http://www.eweek.com/c/a/Health-Care-IT/Hospitals-Must-Seek-Patient-Input-on-EHRs-to-Achieve-Meaningful-Use-PwC-449383/.

electronically, but patients expected access to this information within 30 minutes, PwC reports."[92] Moreover, hospitals are generally ill-equipped to address these needs.

It may well be this final disconnect between the fear of privacy and security breaches on one hand and pressure from consumers and regulators on the other that will result in a new modality for semi-private cloud health care standards. Ultimately the standardization mandated by HIPAA and the pressure to make EHRs subject to an industry certification comparable to PCI certification. Only in this way can the obligations under HIPAA and HHS regulations be met with any sense of confidence by the health care providers.

Conclusion

The growth of cloud computing will diminish the risks for companies that elect to move to the clouds. While the nature of the services vary tremendously and the terms remain only vaguely defined, the transition to SOC 2 and SOC 3 reporting will establish clearer security and privacy practices. The volume of use will help establish the reasonableness of privacy protection for trade secret protection. By carefully reviewing and negotiating the agreements between cloud vendors and their customers, business can gain the benefits of online services while mitigating the risks.

Significant attention must be paid to the particular contractual arrangements afforded by the potential vendor. Absent comprehensive SOC 2 and SOC 3 reports, care must be taken to assure that the agreement provides necessary protection for data privacy, security, reliability, and encryption as well as for personnel selection, training and supervision. And these steps must be ongoing so that the duty to be certified and taking commercially reasonable steps remains an ongoing obligation.

[92] *Id.*

As the levels of risk increases with different types of data, the level of scrutiny necessary increases. Nonetheless, everyone has some of their data in the clouds and must begin paying attention to the benefits and risks associated with these new tools.