

PrivacyTRACKER

iapp

A publication of the International Association of Privacy Professionals

Lost in the Cloud: Suggestions for Navigating Business and Legal Risks in Cloud Computing

Bart W. Huffman, CIPP

Erin Fonté¹

B. Huffman



E Fonté

The shackles are off. In the span of a couple of decades, we have gone from desktop computing – where the user, data, and computing are all together in one physical place – to “cloud” computing – where the user, data, and computing may all be in different physical places, and each may be in more than one place and may move from place to place at any time. Moreover, the setting is global, so the inability of any one nation’s system of laws to keep pace is only the starting point.

This is the information age, and it’s all about access to information and the ability to use and process information. The “right to be let alone – the most comprehensive of rights and the right most valued by civilized men”² has given way to an international community and attention economy in which services are discounted or provided free if the user will agree not “to be let alone.” Fan favorites are global information searching, social and business networking, data sharing, and collaboration tools.

In an effort to address information technology and the information economy, the United States has come up with a multitude of privacy and marketing laws, at the federal and state levels, sometimes on an industry-specific basis.³ Often, companies that do business in a number

See Lost in the Cloud, page 3

¹ The authors acknowledge and appreciate Meagan Gillette, a fellow attorney in Cox Smith’s Privacy, Internet, and Information Technology Group, for her valuable assistance in connection with this article.

² *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

³ The European Union has criticized the United States’ “patchwork of narrowly-focused sectoral laws and voluntary self-regulation [which] cannot at present be relied upon to provide adequate protection in all cases for personal data transferred from the European Union.” Opinion 1/99 of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Jan. 26, 1999, at 2, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp15en.pdf.

In This Issue

Lost in the Cloud: Suggestions for Navigating Business and Legal Risks in Cloud Computing 1

Letter from the Editor 2

Legislative Tracking 11

Credit Agencies & ID Theft 11

Data Security & Breach 11

Government Records, SSN &

Identification 12

Internet 12

Marketing 12

Children & Education 12

Financial, Insurance &

Mortgages 12

Employment 12

Medical 12

Telecommunications & RFID 13

Miscellaneous 13

Legislative Tracking Index 14

Federal Update From Hogan & Hartson 15

Session Calendar 2009 16

Lost in the Cloud

continued from page 1

of states and industries have adopted a policy of complying with all of the various federal and state laws (the “lowest common denominator” approach) in an effort to minimize compliance costs and uncertainty.

By comparison, the privacy paradigm of the European Union differs significantly from that of the U.S. Generally speaking, in the E.U., the baseline is that personal information may not be used or shared, or even transferred, unless the person or a law specifically provides that it may be. This extreme is perhaps just as impractical as that presented by the U.S.. Thus, in an effort to accommodate the global marketplace, including basic operational needs of multinational entities, international legal constructs such as “binding corporate rules” and U.S.-E.U. “safe harbor registrations” have been created and continue to evolve.

Moreover, it should be remembered that the E.U., like the U.S., is a political union with laws at both the federal/union and the member state levels, which many times address intangible rights and assets (and acceptable use and behavior) very differently.

In this setting, it is hard to conceive of the notion of people and businesses storing and processing data in one or more foreign jurisdictions, and accessing that data from interchangeable handheld and desktop devices in one or more different jurisdictions. This, however, is the reality of information technology convergence and the “cloud.”

Cloud Computing

The term “cloud computing” probably has its origins either in telecommunications jargon (where the “cloud” is the unpredictable part of a network) or in the use of a picture of a cloud to indicate the Internet in diagrams. In actuality, the Internet itself is the “cloud,” and people have been doing “cloud computing” since they began using the Internet.

The difference today is that the cloud (i.e., the Internet) is being used more and more by people and companies as the locus of their software applications, data storage, and data processing. Businesses are increasingly looking to the cloud to meet their infrastructure needs, handle their data, and provide “software as a service” (sometimes referred to as “saas”). According to The Economist, in

November 2008, Salesforce.com, one of the largest saas companies, reported “sharply growing revenues and profits”⁴ – a particularly notable accomplishment given the otherwise dismal state of the economy at the time.

Today, individuals compute in the cloud when they use Microsoft’s Hotmail, Yahoo! Mail or Google’s Gmail to send and store e-mail, or when they use Flickr, Snapfish, or Shutterfly to store and share digital photographs, or when they use FlipDrive, Google Docs or DocLanding to remotely store and access Word, Excel or .pdf documents. Interactive, user-controlled social networks such as Facebook and Myspace allow users to create and store content, and even run simple applications, all through their web browser. Most recently, in a move that could threaten the future of operating systems and personal computers as we now know them, Google announced the “GDrive”, which “would follow [the logic of web-based services] to its conclusion by shifting the contents of a user’s hard drive to the Google servers.”⁵

Businesses, on the other hand, compute in the cloud on a macro or enterprise scale, often with information concerning numerous individuals. For businesses, the use of Salesforce’s customer relationship management tools and cloud application platforms, or Amazon’s S3 data storage services, allow them to effectively outsource some of the more costly aspects of business IT needs.

The common “cloud” aspect of these services is that the services and data are accessed through a computer or other device equipped with a web browser, and the bulk of storage and processing comes from centralized data storage and processing centers. And the items stored are not limited to retrieval by the user via a traditional laptop or desktop computer, but may be retrieved by any device capable of establishing a connection to the Internet. With the “cloud,” the individual or enterprise user no longer needs the power of a personal computer or company server – only a web browser is necessary.

Many hardware and service provider companies are investing heavily in projected demand for cloud computing services from individuals and the business world. Below are just a few examples of companies working to develop cloud computing offerings and services.⁶

⁴ *Technology Firms in the Recession: Here We Go Again*, THE ECONOMIST, Jan. 17, 2009, at 62.

⁵ David Smith, *Google Plans To Make PCs History: Industry Critics Warn of Danger in Giving Internet Leader More Power*, THE OBSERVER (Eng.), Jan. 25, 2009, at 22, available at <http://www.guardian.co.uk/technology/2009/jan/25/google-drive-gdrive-internet>.

⁶ See Jeremy Geelan, *Are These the Top 50 Cloud Computing Companies?*, Sys-Con Media (HP), Nov. 11, 2008, <http://hp.sys-con.com/node/665165> (last visited Jan. 26, 2009). The author of this list stated that “[t]he words used to describe the various services and solutions are in every case taken from the [company] Web sites cited” in the article. *Id.*

- 3Tera: provides AppLogic, a cloud computing platform that enables infrastructure solutions that adapt to changing needs of business. According to 3Tera, using AppLogic, IT professionals can: deploy online applications in minutes instead of weeks; scale on demand and deliver security and business continuity for all applications; and be in full control of their cloud environment.⁷
- Amazon: rolled out Elastic Cloud Computing (EC2), an on-demand cloud computing service which allows users to change their capacity requirements for storage and processing. Amazon also offers a Simple Storage Service (S3), a web services interface that offers developers access to the data storage infrastructure that Amazon uses to run its own global network of web sites.⁸
- AT&T: launched a “Synaptic Hosting” initiative for utility computing services, which includes managed networking, security protection and storage.
- Dell: developed Desktoptwo, a “Cloud desktop” offering from Sun Global Partner Sapotek described as “your home in the cloud.” Also developed “Elastra”, which offers to design, deploy & manage database and application infrastructure in the cloud.
- EMC: started a cloud computing division in February 2008. Projects that eventually 85% of all data will be stored in the cloud.
- IBM: provides utility computing services through its beta program Bluehouse.
- Microsoft: developed a cloud computing initiative called Project Azure that is due for release in 2010 and is expected to include a global network of cloud computing servers.
- Rackspace: offers enterprise e-mail management and security services through its Mailtrust service, and on-demand cloud computing services through Mosso.
- Sun Microsystems: operates a cloud computing initiative through Network.com, a part of the Sun Grid project.

The benefits of such cloud computing services are huge. Individuals and small businesses have access to technology that they could not previously afford. Technology providers have new markets, made even more lucrative by the coming-of-age of wireless computing and Internet connectivity of multiple devices. Technology and infrastructure are scalable and, over time, more easily integrated. Updates, upgrades, and error correction can be automatic. Massive

amounts of data can be allocated across multiple servers on a space-available basis, resulting in drastically increased energy efficiency and sharply reduced storage costs. Alternative e-communication methodology and data intensive user content systems (e.g., Facebook and Picasa) have become possible, and e-mail and many other applications are now available for free (other than the “costs” of being subjected to advertisements). And, of course, a “bottomless ocean of information” has become available....⁹

That said, the concerns associated with the cloud are also very real and potentially significant. Aside from the complex, multinational legal issues, one may legitimately question whether handing over responsibility for data security and system reliability to a third party is advisable. Also, as targeted advertising increasingly becomes a primary revenue model for Internet applications, a business or an individual should seek to clearly understand exactly how the data that is submitted to the cloud may be used for the benefit of any third party.

This article focuses on the privacy and data security challenges that are faced, primarily by business (enterprise) customers, in using cloud computing service providers to store and process data in the cloud. Practical considerations are presented at the end of the article for use by businesses in any decision to move data into the cloud and in entering into contracts with cloud computing service providers.

Geographical / Jurisdiction Issues

The virtual programs and data storage in the cloud are accomplished with real, physical machines, and data is stored in a variety of jurisdictions and constantly passing through a variety of jurisdictions.¹⁰ As the Internet continues to grow and evolve, data flows will almost certainly become increasingly unpredictable. In some instances, security concerns further complicate matters, such as when a service provider locates data in multiple jurisdictions as part of its business continuity or disaster recovery plans.

From a privacy perspective, a number of jurisdictions may have significance in determining legal compliance and responsibilities, including: (i) the location of the servers where the data or any copies of the data are stored, (ii) the location of any servers where the data is processed, (iii) the location of the person accessing

⁷ See *Cloud Computing Without Compromise*, 3tera Inc., <http://www.3tera.com/> (last visited Jan. 26, 2009).

⁸ See *Amazon Elastic Compute Cloud (Amazon EC2)*, Amazon Web Services, <http://aws.amazon.com/ec2/> (last visited Jan. 26, 2009), and *Amazon Simple Storage Service (Amazon S3)*, Amazon Web Services, <http://aws.amazon.com/s3/> (last visited Jan. 26, 2009).

⁹ Fred H. Cate, *Information Security Breaches: Looking Back & Thinking Ahead*, PRIVACY & INFO. L. REP., (Thomson/Legalworks, Littlefalls, N.J.), Nov. 2008 (citing David Jones, *Google Is Watching You*, DAILY MAIL, Dec. 1, 2007, at 14).

¹⁰ As of 2008, at least 82 countries had one million or more users of the Internet. *List of Countries by Number of Internet Users*, Wikipedia, http://en.wikipedia.org/wiki/List_of_countries_by_number_of_Internet_users (last visited Jan. 26, 2009).

the service, (iv) the citizenship of the data subject, and (v) the headquarters or regional headquarters of the service provider. The applicable jurisdictions may have special requirements with respect to user-submitted content and the collection, use, and transfer of personal data. Generally speaking, privileges and other statutory protections (such as the U.S. Communications Decency Act, 47 U.S.C. § 230) are only available in the jurisdiction where enacted.

Thus, given that the global community of nations and states is not likely to harmonize its laws concerning Internet data and other intangibles any time soon, an enterprise customer may require disclosure from a cloud computing service provider as to the applicable data storage and processing locations, along with prior notice of any changes to such locations.¹¹ At a minimum, in the absence of such disclosure, it would be difficult to argue that the enterprise customer should assume risks associated with data storage, processing, or transfer involving an unexpected jurisdiction.

Of course, even after the applicable locations are known, the legal consequences remain uncertain. European courts, for example, have found jurisdiction on bases such as the domicile of an executive and the presence of offending material on web servers based in the forum country,¹² and the fact that offensive material could be accessed from within the forum country.¹³ U.S. federal authorities have aggressively sought criminal prosecution against foreign nationals and companies that accept online gambling wagers from persons in the U.S., regardless of where those servers are located.¹⁴

Even among the fifty United States, courts have continued to grapple with applying the traditional principles of personal jurisdiction to the Internet. Courts are turning to factors such as the physical location of servers as well as the state of residence of the service provider in determining where jurisdiction is

proper. For example, in *Verizon Online Services, Inc. v. Ralsky*,¹⁵ the location of the plaintiff-ISP's servers in Virginia factored heavily into the Virginia court's decision to exercise jurisdiction over a nonresident defendant. And in *Facebook, Inc. v. ConnectU LLC*,¹⁶ the state of residence of the online social networking site Facebook was a factor in the court's decision to exercise jurisdiction over a nonresident defendant, even though the defendant was unaware of the actual state of residence.

As a practical and a legal matter, data that is physically located within a jurisdiction may become subject to government or private discovery in that jurisdiction. The U.S., in particular, has received unfavorable attention as a result of increased powers afforded law enforcement under the USA PATRIOT Act,¹⁷ and the Foreign Intelligence Surveillance Act (FISA), as well as instances of perceived abuses of power such as the SWIFT episode.¹⁸ At least for the present, disclosure to persons outside the U.S. that their data will be stored in the U.S. may not be well received.

And such disclosure may be required. The E.U. and its member nations have stringent data transfer and data protection laws. Among other things, enterprise customers must ensure that transfers of data from the E.U. are consistent with their safe harbor registrations and any applicable "binding corporate rules." In addition, notice and permission from the data subjects may be required.

Some cloud computing service providers have taken the position that, because they are U.S.-E.U. safe harbor compliant, their customers are also safe harbor compliant as to data transferred by the service provider within the cloud. Such a position may or may not hold water. As one British commentator observed:

Google Apps is a good example of usable web-based applications. I would guess that most organizations that would make use of this service would have personal information covered under the data protection law passing through it. I

¹¹ Individuals may also expect such disclosure; however, the increasing complexity of the disclosures have led some to question whether linking privacy and security to notice is increasingly unworkable. See Cate, *supra* note 9.

¹² *People v. Somm*, Case 8340 Ds 465 Js 173158/95 (Amtsgericht, Munich, Bavaria 1999). See also Ray August, *International Cyber-Jurisdiction: a Comparative Analysis*, 39 AM. BUS. L. J. 531, 538 (2002), for further discussion on the issue of competing jurisdictions.

¹³ August, *supra* note 12, at 539, 556-57 (discussing anti-Nazi caselaw in which German and French courts found jurisdiction based on accessibility of web based content within the respective countries).

¹⁴ *US Arrest Hits Web Gaming Shares*, BBC NEWS, July 17, 2006, <http://news.bbc.co.uk/1/hi/business/5187520.stm> (last visited Jan. 26, 2009) (reporting arrest in Dallas, Texas of chief executive of online gambling company based in Costa Rica and listed in the London Stock Exchange).

¹⁵ See, e.g., *Verizon Online Services, Inc. v. Ralsky*, 203 F. Supp. 2d 601 (E.D. Va. 2002); see also *America Online, Inc. v. Ambro Enterprises*, 2005 WL 2218433 (E.D. Va., Sept. 8, 2005); *MaryCLE, LLC v. First Choice Internet, Inc.*, 890 A.2d 818 (Md. App. 2006).

¹⁶ See *Facebook, Inc. v. ConnectU, LLC*, 2007 WL 2326090 (N.D. Cal., Aug. 13, 2007).

¹⁷ Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of the United States Code).

¹⁸ In 2006, it came to light that the U.S. government, as part of its efforts against terrorism, had obtained records of the confidential financial transactions of banks, brokerages and stock exchanges from the Society for Worldwide Interbank Financial Telecommunication (SWIFT), which has been described as "the nerve center of the global banking industry." Eric Lichtblau and James Risen, *Bank Data Is Sifted by U.S. in Secret to Block Terror*, N.Y. TIMES, June 23, 2006, at A1.

wonder how many organizations have considered whether this would be legal. As it happens, Google asserts that they comply with safe harbour rules, so it is not a de facto breach of data protection. However, Google can be required to hand over data with a U.S. court order, so there may be sensitive information unsuitable for Google Apps The point is that even with one of the most prominent ‘cloud’ companies around, it can be difficult to pin down the legal ramifications of using their services for business. If utility computing truly turns storage and processing into a commodity (as Amazon S3 and EC2 already does to some extent) then it will become dramatically worse. Having said that, it is not unfixable. Every organization in the E.U. will have the same issue, so standardized schemes for certifying location/jurisdiction/security will be a prerequisite to these services being used in the longer term.¹⁹

Last but not least, a given data location may be associated with certain security risks, such as government unrest or hostility, force majeure events, and criminal acts. In some instances, these risks may be higher in countries that are otherwise attractive as data center locations because of lower labor, energy, and real estate costs. Also, absent appropriate system integrity and business continuity measures, any centralized repository of data may be a prime target for a large-scale cyber-terrorist attack.

Practical Considerations – Choosing to Go to the Cloud

Notwithstanding the unresolved privacy and security concerns, data storage and processing in the cloud offers technological solutions and opportunities that may not otherwise be cost-effective or possible. Through the use of the Internet and cloud technology, businesses can obtain software and services with relatively little up-front investment, and service providers take on tasks such as maintaining servers (in their own data centers), fixing and upgrading hardware and software, and managing disaster recovery planning.²⁰ There is certainly something to be said for placing some aspects of information technology in the hands of companies with true expertise in the field.

In evaluating a cloud computing option, a business should first examine exactly what is being offered from a quality and reliability standpoint. Some questions to consider:

- What “service level agreement” (*i.e.*, the assurance as to up-time availability) is offered, and does the service provider stand behind that assurance with something more than, say, a promise to refund the past month in fees paid to it?
- What is the service provider’s reputation and level of experience in the particular technology being purchased, and in matters affecting data security?
- Is the service provider willing and able to absorb the consequences of data breaches or non-compliance with the law when the service provider is at fault?
- What subcontractors are used by the service provider in connection with handling company data?

On top of these basic concerns, a business should also take a hard look at compliance and security issues. If the business’ customer data is involved, the business should examine its own customer agreement(s) and privacy policy – keeping in mind the limited extent to which any future amendments may apply to existing data. After obtaining information regarding the service provider’s data storage and processing locations, the business should determine what exposure it may face under jurisdiction-specific and industry-specific privacy laws. On this last point, businesses should keep in mind that many of the existing privacy laws were enacted prior to any conception that company data would be stored, accessed, and processed over the Internet using multiple servers in different countries.

In assessing security, a business should be highly skeptical of any cloud computing service provider that is not prepared to address data encryption, firewall, anti-fraud, physical security, background check, access restriction, software reliability, business continuity, disaster recovery, and other such measures. Remember, all security, quality, and reliability concerns that apply to the service provider will also be of concern, and should be addressed, with respect to any of the service provider’s subcontractors that handle any customer data. Some of the questions that should be asked are:

- Where is the data (including backups) going to be hosted?
- Where is the data going to be processed?
- Is strong encryption used for all data transfer and for all data storage?
- What subcontractors will have any access to or control over the data?
- What security guidelines are in place, including background checks?
- Do the security guidelines meet Payment Card Industry (PCI) or any other applicable industry standards?
- What business continuity management systems and disaster recovery plans are in place?

One data security issue that is unique to the cloud computing environment has to do with domain name, or URL, spoofing.

¹⁹ David Evans, *Head in the Cloud, Feet on the Ground*, Unqualified Remarks Blog on British Computer Society Website, June 24, 2008, <http://www.bcs.org/server.php?show=ConBlogEntry.506> (last visited Jan. 26, 2009).

²⁰ Rachael King, *Cloud Computing: Small Companies Take Flight*, BUSINESS WEEK ONLINE, Aug. 5, 2008, http://www.businessweek.com/technology/content/aug2008/tc2008083_619516.htm (last visited Jan. 26, 2009).

Basically, a spoofed URL is one illegitimate website posing as another legitimate website. Spoofing could pose a particularly unique data security risk when a customer's employees believe they are communicating with and transmitting data to a server managed by the service provider, but in reality are sending the information to a server under the control of a cyber thief.

Flaws in [the] DNS [Domain Name System] are giving rise to exploits that could make moving computing functionality into the cloud a risky proposition. Say you're using a software-as-a-service [SaaS] CRM offering. When a salesperson types your SaaS provider's URL, how do you know his browser is linked to the vendor's server, and not to a rogue server? . . . Imagine the damage that could be done in even an hour of employees shipping customer data to a forged site during a busy period for your business."²¹

In order to address this issue, the business customer should inquire whether the service provider has any anti-spoofing verification measures in place with respect to domain name services, given that the business will be accessing its systems and data over the Internet, using IP addresses that may fluctuate while domain names remain constant.²² Although DNS spoofing should set off alarms fairly quickly where there is any typical level of activity, the best security measures in the world are no help if the business user has been routed to an imposter server.

A business should also contemplate whether any amount or type of use of any of the business' data by the service provider will be acceptable. Such use is a common feature of cloud services for individuals such as Gmail, where the individual user receives a seemingly "free" service that is, in fact, paid for by targeted advertising revenues. In the unlikely event that a business would find some amount or type of third party data usage to be permissible in the enterprise cloud context, the business may seek some consideration in the form of additional services or reduced costs. Regardless, this point should be addressed and clearly understood as to all potential mining or other third party uses of company data – whether such use is "anonymous" or not, and whether such use is for direct marketing, one-time targeted advertising, aggregation, quality purposes, or something else.

Ultimately, it may be decided that some of the business' data should not be placed in the cloud, either because of privacy law concerns or simply because the data is too sensitive or confidential to store centrally or to entrust to a third party. In such a situation, it may be worth considering a "private cloud," in which "cloud"-like software can be applied to a dedicated bank of servers.²³

Cloud Computing Service Provider Contracts

Given the often-critical nature of the technology and the amount of data likely to be involved, any proposed cloud computing service provider contract merits close scrutiny. While the service provider may not accept limitless exposure for damages arising from data breach or service interruption, the service provider should accept some responsibility, especially as to matters associated with undisclosed data locations and security issues. Also, the enterprise customer will want to make sure that it retains ownership and a right of access to its data, and that there remains an available avenue for transitioning data back to itself or to another service provider. These and other notable considerations are addressed further below.

(a) *Data ownership and control*

Any business will almost certainly want it to be clear that, as between the business and the service provider, the business owns and retains ownership of its data. But data ownership, the basis of many legal obligations, is not synonymous with data control, which is the true basis of most security risks. Ideally, the service provider would absorb the risks associated with its assumption of control over the data. Practically, however, that is not likely to occur.

Sometimes, neither the business nor the service provider has complete control over the data. Websites built around user generated content (think: YouTube) are classic examples. Such a website (itself technically a cloud computing provider) will not be able to agree to the terms of service of another cloud computing service provider that prohibits certain types of content (pornography, tobacco-promoting, etc.) because the website cannot be sure that its users will not submit such content (even though doing so would contradict the website's own terms of use). As a general matter, businesses should carefully consider whether they can agree to wholesale incorporation of generally applicable or "click-through" style terms of service into their agreement with the cloud computing service provider. While a business may hope that the cloud computing service provider would exercise good judgment before cutting off the business' access to its information or, worse, deleting its data, this issue should be explored and clearly addressed.

Furthermore, as discussed above, the physical location of data under the control of a service provider in a particular jurisdiction may give rise to discovery of that data by law enforcement or private litigants. At a minimum, a business customer would expect notification of such discovery and an opportunity to become involved when legally permissible. Such provisions may be included in the cloud computing service provider's policies. For example, 3Tera includes in its "Acceptable Use Policy" the following provision:

²¹ Mike Fratto, *Locking Down the Cloud: Why DNS Security Must Be Improved*, INFORMATION WEEK, Sept. 27, 2008, at 40, available at <http://www.informationweek.com/news/internet/security/showArticle.jhtml?articleID=210603893>.

²² *Id.*

²³ King, *supra* note 20 (citing NICHOLAS CARR, THE BIG SWITCH 118 (W.W. Norton & Co. 2008)).

Occasionally, 3Tera is required by law to submit customer information to law enforcement officials when presented with a valid subpoena from a court with proper jurisdiction. Information requested is disclosed as directed pursuant to the subpoena. 3Tera utilizes great care in keeping customer information safe and private and will only release information described in the subpoena. 3Tera will notify customer of the information request as allowed by the subpoena.²⁴

This provision, somewhat generously, indicates that the service provider will only respond to “valid” subpoenas issued where there is “proper” jurisdiction (putting some burden on the service provider to assess the validity and enforceability of the subpoenas it receives). For applicable jurisdictions, the business customer will want to think through the various scenarios and make sure that its interests are adequately covered to the extent permissible under the law.

(b) *Data locations and segmentation*

The physical location(s) of data is also significant to an enterprise customer that is concerned about business continuity, security, and compliance. Yet some service providers do not disclose such locations. If the service provider refuses to do so, the business customer simply may not be able to utilize that service provider.²⁵ Otherwise, the business customer can analyze and accept the associated risk, or the business might seek a “private cloud” arrangement or at least an assurance that its data will remain in one country or set of countries (or, conversely, that it will not be stored or processed in certain countries).

Furthermore, a business that decides to put proprietary information in the “cloud” may not want its data stored in the same “cloud” network as its competitors’ data, much less consider the possibility that its competitors may have access to such data. To address such a concern, the service provider might offer data segmentation, which would involve storage of data on networks or servers that are not commingled with a particular company or group of companies.

(c) *Service level agreements*

Service level agreements may address up-time guarantees, service and support levels, and response times. The business customer should examine these assurances not only for what they provide, but also for what remedy is available if they are not met. The service provider’s business continuity and disaster recovery planning should also be taken into account, as it may offer the only truly meaningful remedy.

(d) *Service provider privacy policy / use of data by third parties*

The issue of how the service provider is allowed to access, use or data-mine the customer’s information is a new issue that is fairly unique to cloud computing. The central storage of massive amounts of information has given rise to innovative data mining operations, such as Google’s contextual advertising technology which displays advertisements likely to be of interest to a Gmail user based on a query of the user’s e-mail content.

Specific questions should be posed – especially to companies that are both cloud computing and Web 2.0 players such as Google and Amazon. A business customer will probably wish to impose restrictions on the scanning of documents and other data, including function or activity histories. Also, any advertising injected into a business customer’s cloud-hosted systems should be accompanied by a corresponding benefit. Regardless, the issue of data use by the service provider should be clearly addressed in the service agreement and, if applicable, the service provider’s privacy policy.

(e) *Data security*

A form contract might stipulate that the business customer bears “sole responsibility for adequate security, protection and backup” of its data. Such language may not be appropriate for cloud computing, where the service provider in some respects has almost complete control over security, protection, continuity, backup, and recovery functions.

The allocation of responsibility for security issues should be specifically considered in connection with the service level standards that the business customer requires and the service provider agrees to meet. Given that the service provider is not likely to fully absorb any meaningful component of the risk, the business customer should carefully review the service provider’s security measures, seek audit rights where possible and economically feasible, and may even want to consider an escrow arrangement if the data is essentially irreplaceable or the system is particularly critical.

(f) *Access control procedures*

Another important security related topic is the access control procedures that the service provider implements. For example, are access rights limited, so that an intruder cannot gain access to or delete all or a significant amount of the business customer’s data? Does the service provider employ some type of multi-factor authentication (such as a security token and challenge questions)? Is the password strength and any related password encryption up to industry standards? Does the customer have the authority

²⁴ See Acceptable Use Policy, ¶ 24 Disclosure To Law Enforcement, 3Tera, Inc., <http://www.3tera.com/Terms/Acceptable-use-policy.php> (last visited Jan. 26, 2009).

²⁵ For example, the U.K. Data Protection Act provides that data controllers (with few exceptions) must provide a “notification to the Commissioner” which must include, among other things, “the names, or a description of, any countries or territories outside the European Economic Area to which the data controller directly or indirectly transfers, or intends or may wish directly or indirectly to transfer, the data.” Data Protection Act, 1998, c. 16, §§ 16(1)(f) and 18(1)-(2) (Eng.).

and ability to immediately turn off or block access when the customer terminates an employee? Although these types of issues are common for in-house IT departments, they should not be left behind when a business ventures into the “cloud.”

(g) *Post-termination/transition measures*

Because of the highly valuable nature of some business data, the business customer should review the services agreement for situations where access and a right to return of the data are not absolute. Some service provider contracts exert the right to retain or destroy the customer’s data in the event of termination for breach, including non-payment. Others state that, in the event of termination or expiration for any reason, the customer’s data will be destroyed after a period of days for security and privacy reasons.

From the customer’s perspective, these types of provisions may not be acceptable. If necessary to address legitimate concerns of the service provider, alternative arrangements such as advance payments that get applied to post-termination storage periods and pre-paid transition services should be considered.

(h) *Checklists*

For convenience of reference, some of the factors for a business to consider in evaluating whether to use a cloud computing service are as follows:

- Levels of sensitivity of the data;
- Level of disclosure by the service provider as to data flows, locations, and security measures;
- Compliance with privacy policies and, if applicable, with safe harbor certifications;
- Compliance with data transfer laws and other laws of jurisdictions where the data is going to be hosted or processed; and
- Other potential exposure arising from location of data in a foreign jurisdiction such as: the absence of statutory immunities and protections (such as the U.S. Communications Decency Act and the Digital Millennium Copyright Act), technology transfer laws and import/export requirements, requirements as to user submitted content (e.g., requirements concerning the collection of personal information in connection with content submission), and susceptibility to government or other legal discovery.

In evaluating a prospective cloud computing service contract, a business may wish to consider:

- Responsibility for costs of notification and other expenses or damages in the event of data breach;
- Responsibility for violations of data transfer or other law as a result of location of the data in an undisclosed or unexpected jurisdiction;
- Disclosures and assurances with respect to subcontractors;

- Transition services and data formats and accessibility in the event of a dispute or upon contract termination;
- Audit rights;
- Data and application escrow services;
- Obligations with respect to government or private litigation requests for data; and
- The possibility or need for data segmentation and/or “private clouds.”

Conclusion

When contemplating moving data into the cloud, business customers should compare vendors, read the fine print, involve their lawyers and best technical minds, and think ahead. A customer should manage more tightly the systems and data it cannot afford to be without. Service providers should learn to anticipate the questions and concerns that all businesses will have about moving data into a cloud computing environment, and should be ready to offer explanations, technological solutions and legal provisions to address those concerns. Service providers should also be sensitive to customers in the health, financial, or other heavily regulated industries that face legal requirements to obtain certain promises and assurances from their third party vendors. As cloud computing matures, so will the legal issues that arise out of the business use of the environment. Both business customers and service providers must be prepared to revisit their agreements and practices as this computing environment grows.

Bart Huffman is a shareholder with Cox Smith Matthews, one of the leading business law firms in Texas. Cox Smith Matthews is the largest and oldest firm in San Antonio and has a growing presence in key Texas markets including Austin, Dallas, and McAllen. Bart is an intellectual property attorney who specializes in privacy, data security, information technology, and e-commerce issues, agreements, policies and litigation. An IAPP Certified Information Privacy Professional, Bart is head of Cox Smith’s Privacy, Internet, and Information Technology Group. He is licensed to practice law in the States of Texas, New York, and California, and he is a registered patent attorney and is admitted to practice before various federal courts. Bart has a B.S.E., Civil Engineering & Operations Research, from Princeton University, cum laude, Tau Beta Pi, with a Certificate in Engineering and Management Systems, and he received his J.D. with honors from the University of Texas School of Law. He can be contacted at bhuffman@coxsmith.com.

Erin Fonté is a lawyer with the Austin office of Cox Smith Matthews. Erin’s practice includes a variety of corporate, technology and transactional matters. She focuses on counseling financial services, retail and corporate clients on a variety of issues, including technology issues, information and data management, financial and other privacy issues, compliance with data security regulations, and responses to data breach incidents. Erin is licensed to practice law in the States of Texas and California. Erin has a B.A. in government and philosophy from The University of Texas at Austin, with honors, Phi Beta Kappa, and she received her J.D. with distinction from Stanford Law School, Stanford University. She can be reached via telephone at (512) 703-6318 or via e-mail at efont@coxsmith.com.