Bloomberg Law Reports® Technology Law

Approaching the Cloud: What You Should Know

David G. Rickerby and Christine M. O'Connor, Choate, Hall & Stewart LLP

Cloud computing is a new way to deploy computing technology via the Internet. Although many people may not realize it, most already use cloud computing. Social networks such as Facebook and LinkedIn, as well is Wikipedia, WebMD, Google Apps and Gmail, are all examples of cloud computing. As cloud computing matures, companies are contemplating transitioning certain business functions to the "cloud." Adopting the "cloud" mindset – moving from the idea of company owned and operated software and hardware, towards a utility model, like electricity, where computing is obtained from third parties and consumed on demand – requires feet-on-the-ground risk-benefit analysis. Cloud computing can offer significant value in the form of reduced investments in computing assets and anytime-anywhere access. The risks include potential liability arising from violations of privacy and data security laws and eased access to protected, privileged or trade secret information by the government, adverse litigants or competitors.

What is the current state of cloud computing and what are some of the benefits it offers? Let's look at the potential data risks and ways to reduce these risks.

What is Cloud Computing?

Although definitions vary, generally "cloud computing" is the use of software and data storage applications that are maintained on remote servers owned and operated by third parties and accessed via the Internet. Companies using the cloud "rent" access to powerful applications, platforms and storage areas on an as-needed basis rather than owning and supporting the software and hardware necessary to perform selected business functions on-site. Any information that can be stored locally, such as e-mail, product plans, financial information, sales numbers and health records, also can be stored with a single cloud provider or many.

The cloud itself is a network of data centers or infrastructure shared between and used by unrelated organizations. Some cloud service providers host numerous software applications, while others may provide a single service, such as e-mail. Cloud service providers often offer access to processing power or capacity needed for intensive data manipulation. This is especially useful for one-time only projects that otherwise would require the purchase of high-end hardware and specialized software. Importantly, cloud computing exists in a dynamic environment, where providers frequently leverage their own businesses by building on top of other

---

infrastructure and services available "in the cloud." By combining services, the cloud providers offer the end users (your company) important benefits, including:

Universal Access: All that is needed is an Internet-capable device to access the high-powered computing and data storage of the cloud anytime and anywhere.

Infrastructure On-demand: Rather than owning computing assets that are under-utilized during non-peak periods, outmoded as technology develops or business needs change and limited in processing power, sophisticated cloud platforms allow users to leverage the cloud provider's infrastructure while paying only for the capacity and services consumed.

Economies of Scale: Because cloud services are provided to users of many companies, (1) an individual company's costs for software, data storage and processing is usually reduced significantly, (2) developers of business-specialized applications benefit from access to applications and resources built by others, and (3) multi-site work teams, particularly international teams, can more easily collaborate over a shared platform.

However, because so many services are interwoven, using cloud services frequently results in the company's data flowing across multiple service providers' boundaries. The more a company's data is replicated and distanced from its control, the more vulnerable the data becomes to unwanted disclosure.

What to Watch Out For

As a part of moving forward with cloud computing for any business function, companies need to assess and get comfortable with the privacy and security risks. As a first step, the company should conduct a thorough privacy audit of the data it contemplates transferring to, and maintaining through, cloud computing. Second, based on this audit, the company should seek advice concerning the privacy protection afforded such data under federal and state laws and regulations and, if the cloud service provider is located or stores data outside of the U.S., the laws of other countries.[1] The company also should evaluate the privacy expectations created by its own privacy policies, including website and employee privacy policies.

Privacy and Data Security Law Compliance

Identity theft and data breaches have made headlines and triggered legislative and regulatory action to protect individual privacy interests. Laws and regulations designed to protect private information from public dissemination restrict the collection, processing and transfer of information and may impose notification duties and liability on parties that fail to maintain the security of such information. In addition to the costly remedial actions and sanctions that the privacy laws permit, privacy breaches can lead to even costlier reputation and credibility losses.

In the U.S., a myriad of federal and state laws and regulations, often overlapping and sometimes contradictory, have resulted in a confusing legal landscape. Moreover, technology continues to outpace legislation, making it even more difficult

to anticipate the legal obligations facing cloud computing users. For example, the Electronic Communications Privacy Act ("ECPA"), is premised upon e-mail and the Internet as they existed in the 1980s. The privacy protections available under the ECPA hinge upon undefined distinctions between "electronic communication service" and "remote computing service" and whether e-mail is in transit or stored. Thus, parsing through the statutory obligations often requires understanding the technical infrastructure in use in order to make a best guess as to how dated statutes apply.

Additionally, as part of the analysis, companies must understand the nature of the data they will be sending into the cloud and the legal protections afforded such data. Generally, private data can be divided into three categories for consideration:

- Personally Identifiable Information ("PII") – Many federal and state laws and regulations focus upon information that can be used to identify or locate an individual, such as a person's name combined with his/her address, social security number, credit or banking data, or e-mail or Internet Protocol (IP) address.
- Sensitive Information – Although not as uniformly protected as PII, specific statutes and regulations require information concerning an individual's health, ethnicity, sexual orientation, union membership, criminal history, financial status or job performance be protected.
- Usage Data – Pending legislation and regulations focus upon securing information concerning an individual's behavior such as purchasing patterns tracked by shopping or membership cards or Internet browsing or viewing habits tracked by Local Shared Objects, such as browser cookies, flash cookies and persistent cookies.

Federal privacy laws tend to be applicable to particular types of records or businesses. For example, under the Gramm-Leach-Bliley Act, financial institutions generally cannot disclose personal financial information about consumers and, under the Health Insurance Portability and Accountability Act ("HIPAA"), the use and disclosure of individually identifiable health information is restricted. There are privacy laws directed specifically at tax preparation, bankruptcy matters, student records, cable subscriptions, online browsing by children, identification verification, credit card use and check cashing, video rentals and many other activities. Few of these laws clearly prohibit the use of unaffiliated third party service providers (HIPAA, the Violence Against Women Act and laws directed at tax preparers appear to be the most restrictive), and thus most do not foreclose the use of cloud computing.

The duty to maintain the privacy of these records under these laws, however, largely rests with the party that initially collected the private information. Moving to the cloud does not change that fact. Every company should take appropriate steps to secure information it collects about consumers, employees, potential employees and others that include personally identifiable information. Where such information is used for a business function that the company is considering outsourcing to cloud computing – i.e., human resource functions or customer profile and purchasing records – the company should diligently review the security and safety measures offered by the cloud service provider and assess the risk of a potential data breach.

In addition to assessing potential liability arising from non-compliance with privacy laws or regulations, companies should be cognizant of their own privacy policies. Mistreatment of personal data collected pursuant to published policies can lead to consumer or employee disputes. Thus, before shifting data from in-house servers to a cloud provider, companies should first, review the legal protections at work for the data the company keeps and, second, make sure that the data security and privacy practices in the cloud environment are at least as good as their own.

It is also important to recognize that the location of the cloud provider or, more accurately, the data held by the cloud provider, may trigger privacy protection laws of other countries. For example, under the European Union's Data Protection Directive, the transfer of private personal data without authorization of the individual is highly-restricted. EU member states have a broader definition of private data than that commonly used in the United States and that definition typically includes a combination of PII, sensitive information and usage data. If the cloud provider is located in the EU and data is transferred to the cloud provider, that data may well be subject to the laws of that specific country and the EU rules limiting data transfers to third countries. Thus, even if the information originated in or is being kept on behalf of a U.S. company, the export of the data back to the U.S. after it has been held in the EU could be restricted or prohibited.

Limiting Use of Company Data by the Cloud Service Provider

Many cloud service providers offer their services without individual contracts and subject to published "Terms of Service." These terms may give the cloud provider a variety of rights, including: (1) rights to use, distribute, copy or share information transferred to the cloud by the company; (2) the right to change the terms of service or their privacy policy without limitation and at any time; and (3) the right to terminate its services to the company at any time.

For some business functions, the privacy implications of cloud computing, particularly under the provider's "Terms of Service," are easily identified. For example, the hiring function typically involves an employment application that includes an individual's Social Security number, date of birth and other identifying information. It may also involve background checks, including prior job performance information, credit reports and criminal history checks. Moving this function to the cloud, without first defining information ownership rights and limiting the cloud service provider's rights to use or disclose the private information, could result in the company facing civil, and possibly criminal, liability under one or more federal and state privacy laws.

The risks surrounding other business functions may be less obvious. For example, the use of a cloud service for company e-mail may seem an innocuous decision. If, however, the cloud service provider retains the right to read, use and share information in the company's files, the e-mail may be data-mined for information to be used for secondary purposes. For instance, the cloud provider could derive from e-mail the interests of individuals to target advertising or marketing materials to company customers' or employees' e-mail addresses. Similarly, using cloud computing to facilitate group development of documents concerning a contemplated business venture can be risky if the service provider's motives and rights are not understood. Even if the cloud provider had no access to the substantive information

in those documents, it may be able to derive nearly as much from the transactional information – who had access to a document or data on the cloud and when. This information can expose relationships or transactions that, if revealed, signal the confidential intent of the parties.

An additional concern is that the confidentiality of trade secrets or legally privileged documents may be waived if stored in the cloud, particularly if the cloud provider has retained rights to see, use or disclose information. The Uniform Trade Secrets Act requires reasonable efforts be taken to maintain the secrecy of trade secrets. Similarly, legal privileges, such as the attorney-client or doctor-patient privilege, are premised on the concept of confidentiality. Allowing a cloud service provider to see and use such information may well vitiate any protection against disclosure to others.

Additionally, companies should understand that third party hosts often have less incentive than the company to resist attempts to compel disclosure by government agencies or litigants. Regulators and opponents may seek records from a cloud provider rather than directly from the company. Unless specifically provided for, the cloud service provider is not under an obligation to notify the company that it received a subpoena or provide the company with the time needed to address the subpoena before responding.

Protect Company Information with a Service Agreement

As described above, companies may find that the cloud service provider's boilerplate terms of service and privacy policies are inadequate for certain business functions. However, if the opportunity is sufficient, those terms are usually negotiable and can be superseded. Similarly, service-level agreements can be altered to cover security parameters, infrastructure transparency, and data privacy along with the usual reliability and uptime standards. Note, however, that software and Internet-based businesses do not innately gravitate towards service agreements, as evidenced by the prevalence of "standard" licensing in the software field (often on a shrinkwrap or clickwrap basis) and industry efforts to limit liability under any circumstances.

Any service agreement should specifically address the ownership of the data, the cloud service provider's use, if any, of company information, and the process by which the relationship can be terminated so that substitute computing services can be acquired, company information is returned and company information is removed from the cloud. From the buyer's standpoint, any cloud service agreement should address the following issues:

- The contractual obligation the cloud service provider will assume and the standard of care the cloud server provider will meet to protect company data. This could include reference to particular steps and procedures, including encryption used for both stored data and during transfer of data, two-factor authentication access control, traffic reporting, monitoring services, system failure redundancy and back-up.
- The contractual obligation the cloud service provider will assume regarding uptime, and, if any, whether the cloud service provider will provide an uptime

warranty.

- The company's rights when the agreement ends of it the cloud provider merges or sells its business, ceases business or files bankruptcy, specifically whether the company will have notice in order to obtain new processing services, will the cloud provider assist in transition the company to a new service or back in-house, how the company gets back its data and how the cloud service will remove the company's data from the its and its affiliates' clouds.
- The company's rights if the company is late on payment or withholds payment if dissatisfied with the cloud service provider's performance, including what happens to the company's information and access during such a dispute.
- The remedy limitations, if any. Consider carefully any terms concerning caps on damages, exclusion of consequential damages, exclusion of equitable remedies or other limitations that limit recovery to fees paid.
- Limitations of where company data can be stored, including seeking an agreement to keep the data in a specific location or group of locations, under specified conditions and at agreed security levels. This could be important for regulatory and privacy law reasons, but also for reasons associated with meeting general customer confidentiality obligations or complying with the company's published privacy policies.
- Data and information preservation obligations with respect to regulatory mandates or litigation holds and how, if at all, the cloud service provider will assist the company in meeting these obligations.

David G. Rickerby heads the Technology Transactions & Licensing Group at Choate, Hall & Stewart in Boston. Christine M. O'Connor is an associate at the firm. They can be reached at drickerby@choate.com and coconnor@choate.com.

---

[1] For a fulsome discussion of these issues see Robert Gellman, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, World Privacy Forum (Feb. 23, 2009).