Privacy in the Cloud: A Legal Framework for Moving Personal Data to the Cloud

For many companies, the main question about cloud computing is no longer whether to move their data to the “cloud,” but how they can accomplish this transition. Cloud (or Internet-based on-demand) computing involves a shift away from reliance on a company’s own local computing resources, in favor of greater reliance on shared servers and data centers. Well-known examples of cloud computing services include Google Apps, Salesforce.com, and Amazon Web Services. In principle, a company also may maintain its own internal “private cloud” without using a third-party provider. Since many companies choose to use third-party cloud providers, however, this article will focus on that cloud computing model.

Cloud computing offerings range from the provision of IT infrastructure alone (servers, storage, and bandwidth) to the provision of complete software-enabled solutions. Cloud computing can offer significant advantages in cost, efficiency, and accessibility of data. The pooling and harnessing of processing power provides companies with flexible and cost-efficient IT systems. At the same time, however, cloud computing arrangements tend to reduce a company’s direct control over the location, transfer, and handling of its data.

The flexibility and easy flow of data that characterize the cloud can raise challenging issues related to protection of data in the cloud. A company’s legal obligations and risks will be shaped by the nature of the data to be moved to the cloud, whether the data involve personal information, trade secret information, customer data, or other competitively sensitive information. This article describes the special legal considerations that apply when moving personal information to the cloud. It also offers a framework to help companies navigate these issues to arrive at a solution that meets their own legal and business needs.

DETERMINE THE CATEGORIES OF PERSONAL INFORMATION TO BE MOVED TO THE CLOUD

As a general principle, personal information includes any information that identifies or can be associated with a specific individual. Some types of personal information involve much greater legal and business risks than other types of personal information. For example, a database containing health information will involve greater risks than a database containing names and business contact information of prospective business leads. Also, financial regulators in many countries require specific security standards for financial information. Accordingly, a cloud computing service that may be sufficient for the business lead data may fail to provide the legally required level of protection for health, financial, or other sensitive types of information.

A company will want to develop a strategy that provides sufficient protection to the most sensitive personal information to be transmitted to the cloud. In some cases, a company may elect to maintain certain types of personal information internally, in order to take advantage of more cost-efficient cloud computing services for its less-sensitive data.

IDENTIFY APPLICABLE LAWS AFFECTING YOUR OUTSOURCING OF PERSONAL INFORMATION

Cloud computing, by its nature, can implicate a variety of laws, including privacy laws, data security and breach notification laws, and laws limiting cross-border transfers of personal information.

Privacy Laws

Companies operating in the United States will need to consider whether they are subject to sector-specific privacy laws or regulations, such as the Gramm-Leach-Bliley Act (GLBA) or the Health Insurance Portability and Accountability Act (HIPAA). Such laws impose detailed privacy and data security obligations, and may require more specialized cloud-based offerings.

European-based companies, as well as companies working with providers in or with infrastructure in Europe, will need to account for the broad-reaching requirements under local omnibus data protection laws that protect all personal information, even basic details like business contact information. These requirements can include notifying employees, customers, or other individuals about the outsourcing and processing of their data; obligations to consult with works councils before outsourcing employee data; and registering with local data protection authorities. Similar requirements arise under data protection laws of many other countries, including countries throughout Europe, Asia, the Middle East, and the Americas.

Data Security Requirements

Even if a company is not subject to these types of privacy laws, it will want to ensure safeguards for personal information covered by data security and breach notification laws. In the United States, these laws focus on personal information such as social security numbers, driver's license numbers, and credit or debit card or financial account numbers. One of the key safeguards is encryption because many (although not all) of the U.S. state breach notification laws provide an exception for encrypted data.

In contrast, many other countries require protection of all personal information, and do not necessarily provide an exception for encrypted data. Consequently, companies operating outside of the United States may have broader-reaching obligations to protect all personal information. While data protection obligations vary significantly from law to law, both U.S. and international privacy laws commonly require the following types of safeguards:

- Conducting appropriate due diligence on providers;

- Restricting access, use, and disclosure of personal information;
- Establishing technical, organizational, and administrative safeguards;
- Executing legally sufficient contracts with providers; and
- Notifying affected individuals (and potentially regulators) of a security breach compromising personal information.

The topic of data security in the cloud has received significant industry attention. The National Institute of Standards and Technology (NIST) is working to develop guidelines, and recently issued its draft Guidelines on Security and Privacy in Public Cloud Computing. In the interim, industry groups, such as the Cloud Security Alliance, have suggested voluntary guidelines for improving data security in the cloud. The CSA's Security Guidelines for Critical Areas of Focus for Cloud Computing V.2.1 (December 2009) are available at http://www.cloudsecurityalliance.org/csaguide.pdf. Providers also may choose to be certified under standards such as ISO 27001, although such certifications may not address all applicable legal requirements.

Restrictions on Cross-Border Data Transfers

A number of countries—e.g., all the European Economic Area (EEA) Member States and certain neighboring countries (including Albania, the Channel Islands, Croatia, the Faroe Islands, the Isle of Man, Macedonia, and Switzerland), as well as countries in North Africa, the Middle East, Latin America, and Asia (including Morocco, Israel, Argentina, Uruguay, and Korea)—restrict the transfer or sharing of personal information beyond their borders. These restrictions can present significant challenges for multinational companies seeking to move their data to the cloud. Recognizing these challenges, some providers are starting to offer geographic-specific clouds, in which the data are maintained within a given country or jurisdiction. Some U.S. providers have also certified to the U.S.-European Union Safe Harbor program, in order to accommodate EU-based customers. However, as the Safe Harbor only permits transfers from the EU to the United States, it is not a global solution. Accordingly, a company should assess carefully whether the options offered by a provider are sufficient to meet the company's own legal obligations in the countries where it operates.

To complicate matters, international data protection authorities, particularly in the EEA, have expressed growing doubts about the permissibility of the cloud model for personal information. For example, Mr. Thilo Weichert, the head of the data protection authority of Schleswig-Holstein (one of the smaller German federal states), recently issued an opinion arguing that any cloud located outside the EEA was unlawful unless explicit written (pen on paper) consent was obtained from all of the individuals involved. In Mr. Weichert's opinion, cloud computing was neither "necessary" nor "legitimate" and therefore was forbidden without such consent. See (in German) Thilo Weichert: Cloud Computing und Datenschutz, available at http://www.golem.de/1006/75887.html. Note that the opinion is not legally binding, even for companies established in Schleswig-Holstein, and it appears unlikely that other German federal states (or other data protection authorities in the EEA or elsewhere) will follow this restrictive interpretation. However, the opinion has attracted significant attention and the Working Party 29, the assembly of European data protection authorities, has included cloud computing in its work program. The Working Party 29 is currently expected to issue guidance about cloud computing in 2011.

REVIEW CONTRACTUAL OBLIGATIONS AFFECTING YOUR OUTSOURCING OF PERSONAL INFORMATION

If your company is seeking to outsource to a cloud provider applications that involve third-party data, such as personal information maintained on behalf of customers or business partners, it is important to consider any limitations imposed by contracts with those third parties. Such agreements might require third-party consent to the outsourcing or subcontracting of data processing activities, or may require your company to impose specific contractual obligations on the new provider

or subcontractor.

SELECT AN APPROPRIATE CLOUD COMPUTING SOLUTION

Cloud services tend to be offered on a take-it-or-leave-it basis, with little opportunity to negotiate additional contractual protections or customized terms of service. As a result, companies may find themselves unable to negotiate the types of privacy and data security protections that they typically include in contracts with other service providers. Companies will need to evaluate whether the contract fulfills their applicable legal and contractual obligations, as discussed above. Beyond that, companies will want to evaluate the practical level of risk to their data, and what steps they might take to reduce those risks.

Public vs. Private Cloud

Broadly speaking, a private cloud maintains the data on equipment that is owned, leased, or otherwise controlled by the provider. Private cloud models can be compared with many other well-established forms of IT outsourcing, and do not tend to raise the same level of concerns as a public cloud model.

A public cloud model disperses data more broadly across computers and networks of unrelated third parties, which might include business competitors or individual consumers. While offering maximum flexibility and expansion capabilities, the public cloud model raises heightened concerns about the inability to know who holds your company's data, the lack of oversight over those parties, and the absence of standardized data security practices on the hosting equipment. Given these challenges, companies outsourcing personal information will want to understand whether the proposed service involves a private or public cloud, as well as evaluate what contractual commitments the provider is willing to make about data security.

Securing Data Before Transmission to the Cloud

Companies also may be able to take measures themselves to protect personal information before it is transmitted to the cloud. Some provider agreements instruct or require customers to encrypt their data before uploading the data to the cloud, for example. If it is feasible to encrypt the data prior to transmission to the provider, this may provide substantial additional protections, as long as the encryption keys are not available to the provider.

It is also important to account for applicable security requirements. To this effect, several countries in Europe have very specific statutory requirements for security measures, and some regulators have issued detailed security standards for cloud computing providers, such as the recently published security standards from the German IT-Security Agency. This paper, published on September 27, 2010, sets forth in great detail minimum requirements for cloud computing services, as well as other related services such as IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service). The requirements include specific organizational and technical standards, access controls, encryption, incident response planning, and data portability. The paper is not yet final as the Agency is seeking comments from the industry. See *Bundesamt für Sicherheit in der Informationstechnologie: Mindestsicherheitsanforderungen an Cloud-Computing-Anbieter*, available (in German) by clicking here.

Contract Issues

The contract with the cloud services provider needs to set out clearly the roles and responsibilities of the parties. Unlike many outsourcing arrangements, cloud service contracts usually do not distinguish between personal information and other types of data. These contracts may still include at least basic data protection concepts, even if they are not expressly identified as such. At a minimum, companies will want to look for provisions preventing the provider from using

the information for its own purposes, restricting the provider from sharing the information except in narrowly specified cases, and confirming appropriate data security and breach notification measures. Given the difficulty of negotiating special arrangements with cloud providers, it is important to select a cloud offering that is appropriately tailored to the nature of the data and the related legal obligations. It is likely that as cloud computing matures, more offerings tailored to specific business requirements, including compliance with privacy and similar laws, will be made available to companies.

CONCLUDING THOUGHTS

While cloud computing can substantially improve the efficiency of IT solutions, particularly for small and medium-sized businesses, the specific offerings need to be examined closely. There is no “one-size-fits-all” solution to cloud computing, especially for companies operating in highly regulated sectors or internationally. By understanding their legal compliance obligations, companies can make informed decisions in selecting cloud computing services or suites of services that best meet their needs.