Electronic Commerce & Law Report™

February 3, 2010

Privacy and Data Security Risks in Cloud Computing

by Lisa J. Sotto, Bridget C. Treacy, and Melinda L. McLellan

In recent years, cloud computing has emerged as one of the fastest-growing segments of the information technology industry. The ability to leverage economies of scale, geographic distribution, open source software and automated systems to drive down costs makes cloud computing an attractive option for businesses. But many of the advantages of cloud computing are accompanied by collateral legal and reputational risks. This article outlines U.S. and European Union regulatory requirements applicable to data stored by cloud providers and highlights some of the risks associated with the use of cloud computing.

Overview

As nebulous as its name suggests, the term "cloud computing" has defied precise description by industry experts. Recently, the National Institute of Standards and Technology defined cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources … that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Cloud computing as a product includes a variety of different types of services and infrastructure models, each with its own advantages and disadvantages. For example, companies may employ private clouds, community clouds, public clouds or hybrid clouds to meet their business needs. A key feature of non-private clouds, the pooling of resources using a common infrastructure serving many clients at once, implies both an increased risk of inadvertent or unauthorized access to data by others in the cloud and an inability to pinpoint with any specificity where data resides at a given moment. This ambiguity regarding jurisdictional issues provokes a host of vexing privacy law concerns. Considering the complex regulatory issues surrounding data protection across various jurisdictions, the inability to know where one's data is located, or if and when the data may be moved to another state or country, implies a good deal of potential legal risk.

U.S. Privacy and Data Security Law Issues

Storing data with a cloud provider may trigger numerous state and federal privacy and data security law requirements. Below is a summary of some key U.S. legal and regulatory considerations that may come into play in the cloud computing context.

Service Provider Restrictions

Certain U.S. regulatory frameworks require data owners to ensure that their third party service providers are capable of maintaining the privacy and security of personal information entrusted to them. Often this is accomplished through the use of contractual provisions mandating particular security measures. Two federal privacy laws that restrict the activities of service providers are the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, and the Gramm-Leach-Bliley Act, Pub. L. 106-102, 113 Stat. 1338, codified in relevant part at 15 U.S.C. §§6801-6809 and §§6821-6827. In addition, there are a number of state laws and regulations that impose security-based restrictions on service providers that have access to personal information. While these requirements do not restrict the geographic movement of a company's personal information (unlike the laws in the European Union), they do place restrictions on the use of service providers regardless of where they, or the data, are located.

HIPAA Restrictions on Health Data

Through its Privacy and Security Rules, HIPAA imposes significant restrictions on the disclosure of protected health information. With respect to disclosures to service providers, the regulations require covered entities to enter into business associate agreements containing statutorily mandated language before PHI may be disclosed to a business associate. Accordingly, any HIPAA-covered entity would first have to negotiate and enter into a business associate agreement with a cloud provider before it could store records containing PHI in a cloud computing facility. In some cases, HIPAA's substantive requirements could conflict with the cloud provider's terms of service, and a covered entity would risk a HIPAA violation by using such a provider for data storage.

Gramm-Leach-Bliley Act

For entities subject to GLB, the use of a cloud provider would be subject to similar restrictions. GLB's Privacy and Safeguards Rules restrict financial institutions from disclosing consumers' nonpublic personal information to non-affiliated third parties. Any such disclosures that are permitted under GLB are subject to a host of restrictions under both the Privacy Rule and Safeguards Rule. Pursuant to the Privacy Rule, prior to disclosing consumer personal information to a service provider, a financial institution must enter into a contract with the service provider prohibiting the service provider from disclosing or using the information other than to carry out the purposes for which the information was disclosed. Under the Safeguards Rule, prior to allowing a service provider access to customer personal information, the financial institution must (1) take reasonable steps to ensure that the service provider is capable of maintaining appropriate safeguards (i.e, the entity must undertake appropriate due diligence with respect to the service provider's data security practices); and (2) require the service provider by contract to implement and maintain such safeguards.

State Information Security Laws

A number of states impose a general information security standard on businesses that maintain personal information. These states, which include Arkansas, California, Connecticut, Maryland,

Nevada, Oregon, Rhode Island, Texas and Utah, have laws requiring companies to implement reasonable information security measures. For example, California requires businesses that disclose personal information to nonaffiliated third parties to include contractual obligations that those entities maintain reasonable security procedures. Accordingly, covered businesses subject to the California law must contractually require cloud providers to implement appropriate safeguards.

In 2008, Massachusetts issued regulations (effective March 1, 2010) requiring any person who holds personal information about Massachusetts residents to develop and implement a comprehensive written information security program to protect the data. The regulations impose stringent and comprehensive data security standards on all businesses with Massachusetts consumers or employees. Companies are required to oversee service providers by (1) taking reasonable steps in the selection process to retain providers that are "capable of maintaining appropriate security measures to protect … personal information consistent with [the] regulations and any applicable federal regulations" and (2) contractually requiring service providers to implement and maintain appropriate security measures for personal information. Companies subject to the Massachusetts regulations that are considering implementing a cloud-based solution must determine whether the cloud provider maintains appropriate security measures to protect the data to be stored and verify that the cloud provider's practices would not violate the company's own policies with regard to personal information.

State Breach Notification Laws

The use of cloud computing may raise concerns with respect to U.S. state breach notification requirements. Over 45 U.S. states and other jurisdictions have data security breach notification laws that require data owners to notify individuals whose computerized personal information has been subject to unauthorized access or acquisition. With cloud systems, a data owner may have little or no control over the security of company data being maintained in the cloud, and it would be virtually impossible from a logistical standpoint for a data owner to confirm security conditions at all the server locations that might be used to house the data. Furthermore, it is unclear how, or if, a data owner would be notified by the cloud provider that its data had been subject to unauthorized access or acquisition that could trigger a notification requirement.

Breach Provisions Under HITECH Act

The Health Information Technology for Economic and Clinical Health Act, Pub. L. 111-5, 123 Stat. 258-263, established new information security breach notification requirements that apply to a wide range of businesses that handle PHI and other health data. The regulations apply to all breaches discovered by covered entities and business associates, but include a harm threshold limiting the breach notification requirement to breaches that present a significant risk of harm. Third party service providers (including cloud providers) must notify covered entities to which they provide services of any breaches they discover so the covered entity can comply with the notification requirements. To the extent a HIPAA covered entity discloses PHI to a cloud provider, it risks exposure to federal data security breach notification requirements under the HITECH Act.

European Union Regulatory Issues

Data protection authorities in the European Union recently have paid particular attention to cloud computing, largely in response to inquiries from vendors and prospective users of cloud technology seeking to ensure compliance with EU data protection requirements. Some of the primary legal considerations related to cloud computing in the European Union are outlined below.

Data Controllers and Service Providers

In the European Union, an entity's status as either a "data controller" or a "data processor" is crucial given that the extent of the entity's data protection obligations is dependent on its role. Data controllers determine the purposes and means of the processing of personal data and are responsible for compliance with data protection law, whereas data processors process personal data on behalf of controllers.

With respect to cloud computing, characterization of an entity as a controller or a processor may depend on the type of cloud computing system that is used or on the technical setup of the system. This characterization will determine the liability of the respective parties for compliance with data protection obligations. Further, and perhaps more significantly, a controller remains responsible for discharging data protection obligations even where the data has been outsourced or transferred to a third party—including a cloud vendor—for processing. It is therefore important for a company to undertake a rigorous assessment of its responsibility for the personal data processed by the cloud provider and, if applicable, enter into a data processing agreement requiring the cloud provider to act only according to the company's instructions, to ensure adequate technical and organizational security and otherwise to comply with legal requirements.

International Data Transfers

The restrictions placed on the international transfer of personal data by EU Member States raise particularly troublesome jurisdictional issues in the context of cloud computing. Transfers of personal data outside of the European Economic Area that originate within the EEA are prohibited unless the receiving country provides for an "adequate" level of protection. Currently, the European Commission considers only a handful of countries to provide an adequate level of data protection, and the United States is not one of them. The transfer o f personal data to a country that is not considered "adequate" may be authorized if the data recipient has implemented a legal mechanism providing for an adequate level of protection (such as adherence to the U.S. Safe Harbor Program) or if the data controller can rely on an exception to the prohibition. Such mechanisms are challenging to implement in a cloud context and may require the approval of an EU data protection authority. To seek to address these concerns, some cloud vendors offer segregated EU clouds that keep EU personal data from being transferred outside the European Union.

Legal Bases for Processing Data in a Cloud

Under EU data protection law, organizations that "process" personal data must have a legal basis for doing so; and uploading data into the cloud is considered "processing" in the European Union. Although a variety of possible legal bases exist, in the cloud context, a business most likely would rely on consent of the data subjects, contract fulfillment, or the "balance of interests" test. But obtaining consent inevitably would be burdensome and, in any case, raises significant legal issues in Europe. For example, to be valid under EU law, consent must be freely given, specific and informed. Given the nature of employment relationships, however, under European data protection law, consent is not considered to have been "freely given" in the employment context. To mitigate the uncertainty this creates, an organization could obtain individual employees' consent at the same time as it informs the relevant works council of proposed processing. This process, however, could be so unpalatable as to outweigh the benefits of implementing a cloud-based computing solution.

Information Security Safeguards

EU data protection law requires data controllers to implement appropriate technical and organizational measures to protect personal data against

(1) accidental or unlawful destruction or loss;

(2) unauthorized alteration, disclosure or access (in particular where the processing involves the transmission of data over a network); and

(3) all other unlawful forms of processing.

When applying this broad requirement to cloud computing there are a number of points companies should consider, including the fact that use of a cloud vendor increases the potential for unauthorized disclosure or access. Accordingly, authentication and access safeguards must be robust and provide for an appropriate level of security. Due to the increased level of public access to the cloud, the risk of an information security breach is correspondingly higher, thus the cloud provider should be required by contract to inform data controllers of any data breach incidents.

Rights of Data Subjects

Subject to certain limitations, individuals have a fundamental right under European Union data protection law to access, block, rectify or delete their personal data. Due to the technical set-up of a cloud computing infrastructure, it may be difficult to guarantee that requests for access, blocking, rectification, or deletion are effectively and properly managed. A service provider agreement would have to address this issue specifically.

Works Councils

In the European Union, works councils must be informed of issues affecting working conditions and employee rights, including matters related to employee privacy and data security. In some countries, a formal agreement must be entered into between the employer and the works council.

Depending on the jurisdiction, works councils may be resistant to the introduction of new technologies (such as cloud computing) that could have an impact on employee privacy, and this resistance might manifest itself in the form of efforts by works councils to block the implementation of a cloud computing solution.

Conclusion

Given the rapidly evolving legal landscape in this area, providing guidance to companies venturing into the cloud is a complex matter. Legislatures and regulatory bodies around the world are grappling with the privacy and data security implications of cloud computing, but they have yet to promulgate any actionable requirements or recommendations.

In addition, a host of non-privacy law questions (related to e-discovery obligations, for example), not to mention non-legal concerns such as the difficulties associated with migrating to a cloud provider's architecture and the possibility of service gaps caused by outages, must be explored prior to committing to the use of cloud technology. Companies seeking to implement cloud computing solutions should do so with caution and closely monitor global developments in this area.