BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT



**Cloud Computing**

**Privacy, Security Challenges**

In the world of cloud computing, data is collected for a wide array of purposes, from people in different jurisdictions, and according to the policies of organizations that may differ widely in their business models, culture and technology applications. When data resides and is processed in the cloud, what data protection and privacy laws apply? Is data stored in the cloud transferred internationally? How is that determination made? The authors explain what cloud computing is, how it is used, and delve into some of the special privacy challenges raised by computing in the cloud. They raise a governance model based on the principle of accountability as a possible way forward.

## Privacy, Security Issues Raised by Cloud Computing

BY PAULA J. BRUENING AND BRIDGET C. TREACY

*Paula J. Bruening is Deputy Executive Director of the Centre for Information Policy Leadership at Hunton & Williams LLP. Bridget Treacy is a partner in the London office of Hunton & Williams and leads the UK Information Management practice. Bruening may be reached at pbruening@hunton.com. Treacy may be reached at btreacy@hunton.com.*

In 2008, the term ''cloud computing'' entered mainstream discussions about data protection and privacy. In cloud computing, resources are provided as a service over the Internet to customers who use them on an as-needed basis. Computing services are available through data centers and accessible anywhere, so that the cloud is a single point of access for tools that address all of the customer's computing needs. This approach to delivering computing power and processing has prompted questions about the security and privacy of information in the cloud, as privacy professionals and information technology experts must ensure that

 ISSN 1538-3423

data is protected, even in this new environment. An emerging governance model based on accountability may provide some answers.

The cloud—characterized by large scale complexes for data storage and processing, delivery of software as an online service and leveraged connection of wireless devices to services and applications offered online—promises systemic and economic changes for business. As customers generally do not own the computing infrastructure but access or rent cloud computing services, cloud computing minimizes capital expenditure and lowers barriers to entry. By uncoupling computing tools from physical location, cloud computing enables users to access data and systems regardless of geography or available media.

Whether they are aware of it or not, consumers are already computing in the cloud. According to a study by the Pew Internet & American Life Project, 66 percent of Americans connected to the Web use some kind of cloud service, including storage of computer files and personal photos, online hard drive back up, and Web-based e-mail. Blogs, wikis and social networks—all popular consumer-facing services that enable better collaboration—are cloud based.

Companies are moving to the cloud, and for good reason. Cloud computing makes it possible for companies to relocate their IT and its management and maintenance outside of their organizations. Because payment for many cloud computing services is based on a utility (like electricity, or mobile phone) or subscription model, customers only pay for what they use. Freed from the need to acquire, service and maintain their IT infrastructure, businesses become more nimble, better able to adapt to changing market demands and to take advantage of service more effectively and economically provided by others. Cloud computing empowers companies to redirect resources toward core functions and competencies.

Cloud computing promises not only cost savings and efficiencies, but the ability to expand and enhance services. Health care delivery provides an important example. Cloud computing would allow a number of hospitals to share infrastructure and link systems to reduce costs and increase efficiencies. By pooling various IT resources into the cloud, hospitals could increase utilization as resources would be delivered only when they are required. The cloud also would provide real-time availability of patient information for doctors, nursing staff and support services, not only nationally but regionally, without regard to country borders. Medical professionals would be empowered to access patient information for consultation and research from any Internet enabled device without special software. Major health care institutions, such as the Cleveland Clinic and Kaiser Permanente, have already entered into partnerships with cloud computing providers to begin to move into the cloud.

**Analysts estimate that within the next five years, the global market for cloud computing will grow to $95 billion and that 12 percent of the worldwide software market will move to the cloud in that period. To realize this tremendous potential, business must address the privacy questions raised by this new computing model.**

Analysts find that across industry, online collaboration and enterprise applications such as customer relationship management, supply chain management and enterprise resource planning drive the growth of cloud computing, and estimate that within the next five years, the global market for cloud computing will grow to $95 billion and that 12 percent of the worldwide software market would move to the cloud in that period.

To realize this tremendous potential, business must address the privacy questions raised by this new computing model. Some, including chief information officers, worry whether data in the cloud can be secured and protected in a way that complies with applicable laws, such as the Sarbannes-Oxley Act, which governs corporate financial reporting, and the Health Insurance Portability and Accountability Act, which sets rules for security and privacy of health records. Consumers, too, must be assured that data about them stored and processed in the cloud benefits from the protection of laws and regulations and the promises that companies make. The success of cloud computing may depend upon whether these questions can satisfactorily be answered.

## Special Privacy Challenges Raised by Cloud Computing

***Jurisdiction.*** When data resides and is processed in the cloud, what data protection and privacy laws apply? Is data stored in the cloud transferred internationally? How is that determination made? Cloud computing contemplates the processing of data anywhere and everywhere, across multiple jurisdictions, simultaneously. While most data protection laws and guidance anticipate linear transfers of information, how do these laws apply in the cloud? Depending upon the location of the vendor's servers, traditional approaches such as model contracts or the Safe Harbor program, used to comply with the EU Data Protection Directive (EC/95/46) (the Directive), may not offer a workable solution and, at best, would be cumbersome to implement and maintain.

European controllers processing data in the cloud confront this jurisdictional issue as they are, in any event, explicitly required to ensure adequate protection for data transferred outside Europe for processing. Some European data protection authorities require data controllers to obtain prior consent or a permit before data may be transferred abroad, and typically require a detailed description of the means, purpose and destination of the transfers, as well as details of applicable

  PVLR ISSN 1538-3423

safeguards. European data protection authorities may in some cases take the view that their local laws apply to all further onward transfers of personal data throughout the chain of processing, particularly where data is initially transferred from Europe to the United States under the provisions of the Safe Harbor.

***Security.*** All companies must ensure adequate security for the storage and processing of data, whether they venture into the cloud or maintain traditional processing centers. Companies offering cloud computing models must be able adequately to reassure both CIOs and individuals that data will be safeguarded. Otherwise, consumer may move their data away from companies that use cloud computing and companies will find themselves constrained in their choice of IT services.

Security concerns may be magnified by the dynamic nature of the cloud environment. Indeed, business' ability to benefit from the speed with which the cloud vendors can adjust, develop and change their offerings is one of the cloud's key advantages. That very speed and flexibility may raise concerns that they come at the cost of a certain level of security.

The issue of data security features prominently in a European data protection context, where the data controller remains responsible for the collection and processing of personal data, even where the data are processed by a third party. The EU Directive requires the controller to ensure that any third party processing personal data on its behalf takes adequate technical and organizational security measures to safeguard the data. European data protection law requires a contractual provision in between the controller and processor to this effect, and controllers typically seek to monitor whether this obligation is fulfilled by undertaking an audit or conducting due diligence inquiries. Increasingly, European data protection authorities actively enforce security obligations against controllers, irrespective of whether the data are processed by a third party on the processor's behalf.

Similarly, the Federal Trade Commission has used its authority under the unfairness prong of the FTC Act's Section 5 in enforcing the Safeguard Rule of the Gramm-Leach-Bliley Act to determine whether a company's information security measures were reasonable and appropriate under the circumstances. The Safeguards Rule requires companies to develop a written information security plan that describes their program to protect customer information. Under both European and United States law, users of cloud computing services will need to identify reliable ways to gain assurance that personal data is secured and protected.

***Fair Information Practices and International Data Transfer.***

The ability to comply with fair information practices is critical to the ability of companies to fulfill legal requirements and meet the promises they make to consumers in their privacy notices. To maintain trust, users of cloud computing must assure customers and regulators that they meet their obligations under law, regulation and the provisions of their privacy policies.

Companies must be certain that consumer choices about the use of their information are respected in the cloud environment. Data in the cloud must be used for the purpose for which it was collected, and onward transfer or other third party use of the data must occur only when authorized by law, as provided for in the terms of the privacy notice, or according to customer preference. When access is offered to the consumer, it must be available to him or her in a reasonably convenient way even in the cloud. Fair information practices as articulated in data protection law in Europe also often require that a controller inform individuals of the fact that their data will be processed abroad—a likely scenario when cloud computing services are used.

**The extent to which companies will outsource their computing to "public" clouds may depend upon the ability to address security concerns.**

Companies from industry sectors ranging from financial services and telecommunications to government and high tech are taking important steps to build internal or private clouds to consolidate their data and IT centers. The extent to which companies will outsource their computing to ''public'' clouds may depend upon the ability to address security concerns, and to ensure that requirements of fair information practices are met.

## Accountability as a Possible Way Forward

Cloud computing would be well served by an emerging privacy governance model based on *accountability*. Accountability requires that business actively take ownership of the responsible management of their information, no matter where it resides or is processed. Accountability does not substitute for data protection or privacy law. An accountable organization complies fully with applicable laws and regulation governing the collection and use of data. But it goes further, putting in place sound information management and privacy practices that enhance the development and protection of the business' brand, reputation and relationship with its customers.

In the world of cloud computing, data is collected for a wide array of purposes, from people in different jurisdictions, and according to the policies of organizations that may differ widely in their business models, culture and technology applications. Information processed in the cloud that is governed by an accountability model will be subject to obligations to secure and process the information in accordance with law, regulation and the collecting company's promises to individuals. At no time do accountable companies relinquish their responsibility to protect information. Rather, they take measures to ensure that the obligations that attach to data—whether through law, regulation or company policies and promises—are met by whomever and in whatever jurisdiction the information is processed. Accountable companies require strong contractual assurances from cloud computing vendors that they are capable of meeting those obligations and safeguarding personal data.

The principle of accountability is not new, though its application may be. The Organization for Economic Cooperation and Development Guidelines' accountability principle makes a data controller accountable for complying with measures that give effect to the rest of the guidance. The Asia Pacific Economic Cooperation Framework articulates the accountability principle more explicitly than provided for in the OECD Guide-

lines. The Canadian privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA), includes accountability as its first principle, and Canadian Privacy Commissioner Jennifer Stoddart recently released guidance about accountability in data transfers. A similar concept underpins the European Commission's Binding Corporate Rules mechanism governing the international transfer of European personal data within a multinational company. But while accountability is a well established principle of data protection law and guidance, little has been written to elucidate what an organization must do to be accountable, or how an accountability mechanism might resolve jurisdictional and local law issues.

In 2009, privacy protection agencies, consumer advocates, business and regulators will undertake a project to define how a company establishes its ''accountability'' credentials, whether information is processed in-house, across the globe, or in the cloud. Technology companies that provide cloud-based services and the businesses that use them will observe these emerging discussions of accountability governance with great interest. Both share a critical objective: to ensure that this new governance paradigm can safeguard data, and privacy, even in the cloud.

  PVLR ISSN 1538-3423