Cloud computing — data protection concerns unwrapped

Bridget Treacy, Partner at Hunton & Williams, and Paula Bruening, Centre for Information Policy Leadership, explore the potential impact for privacy strategies of cloud computing technology

During 2008, the term 'cloud computing' moved into the mainstream. But how many of us really know what cloud computing is? Some mutter the phrase in the same breath as issuing dire warnings for the future of privacy, but does cloud computing really promise to subvert the privacy agenda? Or does this technology herald yet another step in our technological evolution, requiring privacy professionals, as for all new technologies, to identify and assess implications for privacy in the ordinary way?

What is cloud computing?

Cloud computing is not clearly defined. While some use the term to describe what is essentially a distributed computing model, or software-as-a-service, ('SaaS'), most experts agree that true cloud computing encompasses much more. The cloud is 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. It promises system and economic changes for business. Cloud computing makes it possible for businesses to relocate their IT functions to outside of their organisations, so that data storage and processing takes place on the internet, rather than in a data warehouse. Freed from the need to buy, service, and maintain their IT infrastructure, businesses will become more nimble, better able to adapt to changing market demands, and to take advantage of services more effectively and economically provided by others.

Why do companies want to buy services in this way?

Cloud computing is both an IT director's dream and nightmare. On the one hand, a considerable amount of IT infrastructure can be outsourced to the cloud, at significant cost saving. Rapidly growing companies, or those whose demand for IT resources vary, may find cloud computing an attractive option. This is because it offers businesses an unprecedented degree of flexibility by readily scaling up and down the supply of IT services. An organisation pays only for the computing power it uses; therefore, cloud computing releases resources that may then be applied to a business' core functions and competencies.

On the other hand, the extraordinarily rapid evolution of the cloud environment challenges the ability for organisations to maintain consistent security standards, or to provide for adequate back-up and business continuity. Some query whether and, if so, how, the cloud can ever be regulated. Of course, cloud computing raises privacy concerns, described in more detail below.

Are data safe in the cloud?

One of the key consumer concerns raised by cloud computing is whether their data, processed in the cloud, are safe. Security considerations will touch all data in the cloud, but particularly financial and health data. Unless companies providing or using cloud computing models can adequately reassure individuals that their data will be safeguarded, consumers may not permit their data to be processed in this way, and businesses may find themselves constrained in their choices of IT services. However, security and trust related to data processing are issues with which businesses must deal, irrespective of whether they venture into the cloud or adopt firmly terrestrial processing practices. Part of the security concern relates to the fact that cloud computing is a dynamic environment. Indeed, one of its key advantages is that it permits business to benefit from the speed with which cloud vendors can adjust, develop and change their offerings. However, there are concerns that such speed and flexibility come at the cost of compromise to security, possibly to an unacceptable degree.

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 Data Protection Directive (EC/95/46) (the 'Directive') requires the controller to ensure that any third party processing personal data on its behalf takes adequate technical and organisational security measures to safeguard the data. European Data Protection law requires a contractual provision to this effect, between the controller and processor, and controllers typically seek to monitor whether this obligation is fulfilled by undertaking an audit or conducting due diligence inquiries. Seeking reassurance in

(Continued on page 14)

(Continued from page 13)
the environment of cloud computing presents significant challenges, especially where the vendor is small or unproven. Smaller vendors, based outside Europe, may not even be aware of the requirements of the Directive.

Of course larger, more sophisticated vendors who have embraced the cloud model are acutely aware of the need to ensure that data processed in the cloud are adequately safeguarded. Their documentation increasingly reflects these issues, and many vendors proactively highlight them to reassure prospective clients.

To tell or not to tell

Security is not the only data protection issue which will be of interest to privacy professionals seeking to work with their businesses to take advantage of cloud computing. More generally in Europe, regulators promote fair information practices as a means of protecting consumers. Consumers want to know how their data are processed. Transparent data handling practices create trust and enhance brand and reputation.

The Walport/Thomas Data Sharing Review ('the Review'), published in the UK in July 2008, and largely affirmed by the Ministry of Justice ('MoJ') in November 2008, singles out fair information practices for particular comment. The MoJ's response to the Review indicates that fair information practices will receive further attention by the UK Information Commissioner's Office. The Review specifically mentions the need for clear privacy notices that inform people of what data will be processed, by whom and for what purpose. In addition, the MoJ endorsed a recommendation that organisations specifically inform individuals that their data will be processed by a third party.

Considering whether and, if so, how such fair information practices might be promoted within a cloud computing environment raises difficult issues. It may not be practically possible to determine where the data are processed other than that the processing takes place somewhere within the cloud. Indeed, where subcontractors are engaged, it may be difficult to know who actually processes specific data.

Enforcing fair processing obligations may also be difficult where processing takes place in the cloud. Just as the internet challenged our thinking about how we enforce obligations within and across jurisdictions, so the evolution of the cloud challenges our traditional thinking about jurisdiction over data protection issues and the enforcement of breaches.

'Transferred' internationally?

How might the Directive's requirements restricting the international transfer of personal data be implemented where data are processed in the cloud? True cloud computing contemplates the processing of data anywhere and everywhere, across multiple jurisdictions. Bearing in mind the linear nature of data transfers envisioned by existing European data protection laws, how can an EU-based controller ensure compliance where data are processed by a vendor operating in the cloud? Depending on the location of the vendor's servers, model contracts or safe harbor may not provide a workable solution and, at best, will be cumbersome to implement and maintain. Binding Corporate Rules, on the other hand, remain, at best, a long term solution for all but the most determined companies. In practice, solutions to these issues are still being created, but some cloud vendors are able now to offer solutions that permit EU data to remain within the EU for processing.

Time for a new data governance model?

But is the creation of an 'EU cloud' an appropriate solution? Data protection concerns are not limited to Europe, and many good data protection practices are found outside the EU. Some cloud vendors have begun to explore fundamentally different ways to address privacy concerns, developing a data governance model based on the concept of 'accountability'. However, accountability is not a substitute for data protection laws. It requires that businesses actively take ownership of information management. It is a mindset or attitude that values good data protection practices as fundamental to a business' brand, reputation, and relationship with its customers. An accountability model does not dilute or abdicate responsibility for safeguarding personal information. Instead, the business ensures that obligations to safeguard the data are observed by all who process it, irrespective of where that processing occurs.

In the world of cloud computing, data are collected for a wide array of purposes, from different jurisdictions, and under policies of organisations 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. Accountable companies take measures to ensure that obligations attach to data and that these obligations are met by whomever and in whatever jurisdiction the information is processed. Accountable companies require strong contractual assurances from companies providing cloud computing services that they are capable of meeting those obligations and of safeguarding personal data.

These ideas may not be far from becoming a reality. The concept of accountability underpins the EU Binding Corporate Rules mechanism. Further, the Asia-Pacific Economic Cooperation ('APEC') based its framework for protecting information shared within the region on the concept of accountability. The APEC approach provides that organisations that collect personal data remain responsible and accountable for meeting the requirements of the laws, rules, and promises associated with the data, wherever and by whomever the data are processed. Privacy professionals will be expected to identify and assess implications of cloud computing for privacy which arise from this model, in the ordinary way. As the cloud model becomes more widely adopted, the data protection issues raised by the cloud may stimulate wider discussion of the need for a new data governance model, perhaps incorporating in a more direct way the concept of accountability.

Bridget Treacy and Paula Bruening
btreacy@hunton.com
pbruening@hunton.com