Cloud Computing: Plan for Storms

By Timothy M. Banks

ISTOCKPHOTO.COM

The Promise and the Challenge

Organizations are able to leverage reliable internet connectivity to access quickly scalable computing power, platforms and software owned and managed by specialist third parties.

The opportunities presented by these cloud computing technologies were recently acknowledged by the European Commission in its paper *Unleashing the Potential of Cloud Computing in Europe* (available at http://ec.europa.eu). In that paper, the European Commission stated that it "aims at enabling and facilitating faster adoption of cloud computing throughout all sectors of the economy" (public and private) in order to accelerate productivity growth and competitiveness.

There are, however, organizational risks to outsourcing the processing and storage of data to third parties. In addition, cross-border transfers may involve exposure to access by foreign governments, which may pose particular concerns with respect to public sector bodies.

Contract Considerations

In its most complete form, the platform, software, processing and storage of data is provided in a multi-tenant environment owned and operated by one or more third parties on servers distributed in more than one location around the world. A cloud service provider may also provide additional services, such as analytics and data mining services, for the organization.

This creates a number of challenges to the cloud computing arrangement:

- **Ownership.** Negotiating uncontested ownership to the data provided by the organization should not be problematic (at least as between the organization and the provider), although a cloud service provider may need to license use of the data for certain additional services being provided. However, ownership of derivatives of that data created through the cloud services (including analytics), as well as usage statistics and transaction histories of users and other metadata created by the cloud computing arrangement, may prove more complicated. The organization's privacy obligations and intellectual property rights with regard to any data to which the cloud service provider has rights to use or retain independently of providing the services to the organization must also be analysed.

- **Integrity.** A shared, multi-tenant environment introduces new data integrity risks, including (a) commingling of data from different organizations; and (b) visibility of data or usage patterns by another organization. Working with a provider who has been certified to internationally accepted standards may assist in ensuring that the system offers (i) sophisticated partitioning; (ii) a robust alert and auditing process for unauthorized access, deletion or modification of data; (iii) the capability to establish the integrity of the cloud services in order to satisfy Canadian laws with regards to the admissibility of electronic records as evidence.

- **Loss.** The cloud environment introduces new variables, such as: (a) hacking by a tenant sharing the system; (b) the introduction (deliberately or inadvertently) of malicious code by another tenant; (c) insolvency of the provider; and (d) inadequate third-party disaster recovery. An organization should therefore: (i) consider data encryption in transit and at rest (i.e. when stored); (ii) maintain a robust authentication program and encryption/decryption key management system that limits the cloud provider's access to an organization's data; and (iii) ensure a sophisticated disaster recovery plan and contingency plan in the event of supplier insolvency, taking into account that the data may be in foreign jurisdictions and/or in a multi-tenant environment.

- **Lifecycle.** Cloud computing may complicate an organization's data retention and destruction practices if the organization is not in control of the data. The organization should consider: (i) provisions for data portability to a new provider; (ii) protocols for implementing the destruction of data in accordance with the organization's retention periods or upon transfer to another cloud service provider; (iii) capacity to implement a litigation hold to isolate and preserve electronic evidence; and (iv) survival of covenants if the cloud service provider retains any of the derivative data or metadata.

International Transfers

Cloud computing in Canada commonly involves international transfers of the organization's data. There is a risk of foreign government intrusion, depending on a number of factors including the type of cloud service and the type of data involved.

There is no express prohibition of international transfers of data in Canada, with two exceptions: British Columbia and Nova Scotia both prohibit public sector bodies from transferring personal information outside of Canada (or accessing it from outside Canada) without the written consent of the individual. Nova Scotia also prohibits service providers from transferring personal information outside of Canada that is entrusted to them by public sector bodies. It should be noted, however, that Alberta does not expressly permit a public sector body to disclose personal information in response to a foreign subpoena, warrant or order and Quebec's private sector privacy legislation prohibits international transfers of personal information if that personal information might be disclosed to third parties without the consent of the individual. Moreover, some public bodies will be subject to guidelines discouraging or prohibiting processing and storage of data for reasons of national security or policy.

However, it is important to keep the risks of foreign intrusion in perspective. Much has been made of the powers granted to U.S. law enforcement officials, under the USA Patriot Act, to obtain access to data. However, Canada and other countries have similar provisions for law enforcement agencies. The federal Office of the Privacy Commissioner, and more recently the Ontario Information and Privacy Commissioner, have noted that law enforcement agencies in the U.S. and in other countries already have the ability to obtain information through Canadian officials under mutual assistance agreements. The mere potential for foreign governmental access does not (except as described above) make international transfer of data unlawful. This view has been recently echoed by the European Commission in its cloud computing strategy.

Nevertheless, an organization remains accountable under Canadian law for personal information notwithstanding its transfer to a foreign jurisdiction. Organizations are required to provide for comparable levels of protection against unauthorized use, access or modification by ensuring that the service provider contracts contain meaningful technological, physical and administrative security obligations and that compliance with these obligations are audited and enforced. Moreover, organizations must assess the risks posed by the laws or governmental practices of the foreign jurisdiction to determine whether the data will be afforded similar protections. An organization transferring highly confidential information or sensitive personal information will want advice on whether the jurisdiction will afford them with remedies to prevent unauthorized use, access or modification of data and recover/re-secure data if security is breached.

Finally, reasonable people may differ on whether their personal information should be directly subject to foreign laws. Cloud computing almost always necessitates revisions to privacy policies, since individuals should be informed of the cross-border transfer of personal information and, in Alberta, such disclosure is expressly required in the private sector. ■

Timothy M. Banks is a data governance lawyer at Fraser Milner Casgrain LLP. He advises clients on privacy, social media, records-retention, access to information and cross border transfers of information.

Cloud Computing Models

There are three basic types of cloud computing outsourcing that can be provisioned in three types of models.

- Infrastructure as a Service (**IaaS**): outsourcing computing power and storage capacity.
- Platform as a Service (**PaaS**): outsourcing the platform (operating system, application execution environment and database) on which the organization can run software applications of its choosing.
- Software as a Service (**SaaS**): outsourcing the software applications so that the entire computing environment is outsourced.

The three models of cloud computing:

- **Private Clouds:** deployment of services on infrastructure resources dedicated entirely to one organization on a private network.
- **Public Clouds:** deployment of services on shared resources among different organizations.
- **Hybrid Clouds:** combination of deployment methods for different aspects of the system. ■