

Privacy in the Cloud: points to consider

What does cloud computing mean for privacy? 16 points to consider. By **Annelies Moens**.

Cloud computing is essentially a term given to some new information technology services provided over the Internet. These can include storage of data, provision of software and infrastructure as a utility.

Cloud computing enables organisations to outsource many of their computer processing needs thus removing the burden of having to install, maintain, upgrade, store and manage their own data, software or infrastructure. Unlike outsourcing, a cloud computing service provider may host and/or process data across a myriad of computers (not just those owned by the cloud computing service). In some situations, this can provide great cost savings to organisations as they can downscale their in-house information technology staffing, storage, software and infrastructure costs.

The rise of cloud computing can be attributed to several factors, including:

- The extensive networking capabilities of the Internet;
- Technology companies wanting to offer software as a service rather than as a licensed product;
- Organisations not wanting to invest in the next generation of internal processing power; and
- Technology companies developing economies of scale in order to provide cloud computing solutions.

A recent example of the use of cloud computing in Australia is the outsourcing of email accounts and their associated storage requirements on the cloud. Technology providers, such as Google and Microsoft are providing clients, including government agencies and universities, with cloud computing solutions to host their email accounts and storage needs on the cloud. In recent months, there has been a spate of universities in Australia transitioning their staff and student email accounts to the cloud.

In the global commercial sector, an international not-for-profit cross-industry forum (TM Forum) has been estab-

lished to focus on enabling best-in-class IT for service providers in the communications, media and cloud service markets. Large corporations have formed an Enterprise Cloud Buyers Council to work together to ensure an optimal, efficient and flexible cloud computing supplier service market. The Enterprise Cloud Buyers Council intends to develop standards for cloud computing to ensure effective adoption of cloud computing on a global scale, for example by:

- identifying common commodity processes that are best suited to a service type model – where organisations pay for what they consume;
- enabling benchmarking of services across providers, such as Google, Microsoft, Amazon and other cloud computing service providers;
- achieving transparency of costs, service levels and reporting requirements.

It is imperative that, as standards are being formed, privacy professionals contribute their expertise in the management of information to ensure that personal information management practices are not compromised, as organisations move into cloud computing arrangements.

There are a number of privacy questions that we need to address when assessing the business case and risks of entering into cloud computing arrangements that extend beyond traditional outsourcing risks.

TYPE OF DATA AND POLICIES

- 1 How sensitive or critical to your organisation is the data that the cloud provider will be processing/ hosting?
- 2 Whose privacy policy is the data subject to – the client's or the cloud service provider's privacy policy?

DATA LOCATION AND RETENTION

- 3 Where will the data and backups be stored? Will it be stored with other clients' data? Will it be located in politically and environmentally stable regions, for example, not prone to earthquakes?
- 4 What legal jurisdiction(s) will the data be located in?
- 5 What are the data retention policies of

the cloud service provider?

- 6 How does the cloud service provider keep track of where data is stored/ processed? How does the provider ensure that information is protected?
- 7 Is the data encrypted during storage? Who controls the encryption keys: the client or the cloud service provider?

TRANSFERRING DATA

- 8 What security mechanisms are in place to transfer the data between the organisation and the cloud service provider, for example, is it encrypted during transfer? Who controls the encryption keys, the client or the cloud service provider?
- 9 What happens when the data cannot be accessed or retrieved due to technical or other difficulties?

PRIVACY BREACHES

- 10 How will you know if the data has been accessed or used inappropriately?
- 11 What happens when there is an unauthorised breach of privacy and data has been inappropriately accessed, used or compromised?
- 12 Does the provider have sufficient resources or insurance to cover the costs of catastrophic privacy breaches?
- 13 What privacy response and contingency plans are in place at the provider and client to deal with public relations issues and brand damage that may arise if there is a breach of privacy? Are those policies complementary?

CHANGING PROVIDER

- 14 What happens if the cloud service provider ceases to exist?
- 15 Can upgrades to software or other services be refused?
- 16 Can the data be easily relocated if necessary? Can the data be migrated easily to another service provider?

INFORMATION

Further information about TM Forum and the Enterprise Cloud Buyers Council can be found at: <http://www.tmforum.org>.

AUTHOR

Annelies Moens is External Relations Manager, Australasian Legal Information Institute, Sydney (www.austlii.edu.au). Email: a.moens@lycos.com

Your Newsletter Subscription Includes

e-Newsletter

1. Six Newsletters a year

The *Privacy Laws & Business (PL&B) International Newsletter*, published since 1987, provides you with a comprehensive information service on data protection and privacy issues. We bring you the latest privacy news from 50 countries – new laws, bills, amendments, codes and how they work in practice.

2. Helpline Enquiry Service

Subscribers may telephone, fax or email us with their questions such as: contact details of Data Protection Authorities, the current status of

legislation and amendments, and sources for specific issues and texts.

3. Email updates

We will keep you informed of the latest developments.

4. Index

Subscribers receive annually a cumulative Country, Subject and Company index. Multiple headings include advertising, data security, Internet, police, transborder data flows and sensitive data. The index is updated after every issue on our website www.privacylaws.com.

Electronic Option

The newsletter is available in PDF format either for use in one office or for uploading onto your Intranet or network.

This format enables you to see the Newsletter on any computer on your network as it appears in the paper version. It allows you to print out pages at any location.

Privacy Laws & Business has clients in over 45 countries, including 25 of the Global Top 50, 24 of Europe's Top 50, 25 of the UK's Top 50 in the Financial Times lists; and 10 of the Global Top 20 in the Fortune list.

Privacy Laws & Business also publishes the United Kingdom Newsletter, a publication, which ranges beyond the Data Protection Act to include the Freedom of Information Act and related aspects of other laws.

Newsletter Subscription Form

Subscription Packages

(Please add 17.5% VAT to prices for the PDF format within the EU).

- Print** **PDF** (please tick preferred delivery format)
 Send a FREE sample of the *UK/International* newsletter
 PL&B International Subscription **£375**
 UK/International Combined Subscription **£595**
or an extra **£310** for existing UK subscribers)
 Special academic rate – 50% discount on above prices

Multiple Subscription Discounts

- 2-9 copies: 30% discount (indicate no. of copies ...)

Intranet Enterprise Licence for uploading onto your network (including additional printed copies)

- PL&B International* **£1,875**
 PL&B UK **£1,425**
 Both *International/UK* newsletters **£2,975**
 I wish to receive *PL&B's* FREE email news service

Data Protection Notice: *Privacy Laws & Business* will not pass on your details to third parties. We would like to occasionally send you information on data protection law services. Please indicate if you *do not* wish to be contacted by: Post Email Telephone

Name:

Position:

Organisation:

Address:

Postcode: Country:

Tel:

Email:

Signature:

Date:

Payment Options

Address of Accounts (if different):

.....

Postcode:

- Purchase Order
 Cheque payable to: *Privacy Laws & Business*
 Bank transfer direct to our account:
Privacy Laws & Business, Barclays Bank PLC,
355 Station Road, Harrow, Middlesex, HA1 2AN, UK.
Bank sort code: 20-37-16 Account No.: 20240664
IBAN: GB92 BARC 2037 1620 2406 64 SWIFTBIC: BARCGB22
Please send a copy of the transfer order with this form.

- American Express MasterCard Visa

Card Name:

Credit Card Number:

Expiry Date:

Signature: Date:

I am interested in:

- Consultancy/Audits
 In-House Presentations/Training
 Recruitment Service

Please return to: Newsletter Subscriptions Department, Privacy Laws & Business, 2nd Floor, Monument House, 215 Marsh Road, Pinner, Middlesex HA5 5NE, UK, Tel +44 20 8868 9200
Fax: +44 20 8868 5215, email: info@privacylaws.com 16/6

www.privacylaws.com

Guarantee

If you are dissatisfied with the newsletter in any way, the unexpired portion of your subscription will be repaid.