Privacy, the Cloud and Data Breaches

Annelies Moens
Head of Sales and Operations,
Information Integrity Solutions
Legalwise Seminars
Sydney, 20 March 2013
About IIS

Building trust and privacy through global thought leadership and consultancy work for a range of public and private organisations

Services: privacy governance & strategy, privacy impact assessments and audits, regulator, customer & stakeholder engagement, identity management, privacy training.....
Overview

- Changing privacy regulation across the globe
- Cloud computing & privacy risks
- Safeguards
- Data breaches
Australia & New Zealand

Australia:
- Privacy Amendment (Enhancing Privacy Protection) Act 2012 received royal assent in December 2012
- Act to commence in March 2014 – 15 month implementation window

New Zealand:
- Law Commission recommends reform of Privacy Act and progress underway

Building trust and innovative privacy solutions
<table>
<thead>
<tr>
<th>Country</th>
<th>Law / Guideline</th>
<th>In Force</th>
<th>Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malaysia</td>
<td>Personal Data Protection Act, 2010</td>
<td>Not yet</td>
<td>Private sector, in commercial transactions</td>
</tr>
<tr>
<td>Singapore</td>
<td>Personal Data Protection Act 2012</td>
<td>Yes, in phases</td>
<td>Private sector</td>
</tr>
<tr>
<td>Vietnam</td>
<td>Law on Protection of Consumer’s Rights, 2011</td>
<td>Yes</td>
<td>Private sector, in commercial transactions</td>
</tr>
<tr>
<td>Taiwan</td>
<td>Personal Data Protection Act, 2010</td>
<td>Yes</td>
<td>Public and private sectors</td>
</tr>
<tr>
<td>India</td>
<td>Information Technology Act, 2000 and IT Rules, 2011</td>
<td>Yes</td>
<td>Private sector</td>
</tr>
<tr>
<td>South Korea</td>
<td>Personal Data Protection Act, 2011</td>
<td>Yes</td>
<td>Public and private sectors</td>
</tr>
<tr>
<td>Philippines</td>
<td>Data Privacy Act of 2012</td>
<td>Yes</td>
<td>Public and private sectors</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>Personal Data (Privacy)(Amendment) Ordinance 2012</td>
<td>Yes, in phases</td>
<td>Public and private sectors</td>
</tr>
</tbody>
</table>
Finalisation of the Cross-Border Privacy Rules (CBPR) system for APEC member economies

System to ensure that a company’s privacy practices meet established standards for the protection of personal information

First participant of CBPR is USA, then Mexico, with more to follow, including Japan this year

Discussions to foster interoperability with the EU’s Binding Corporate Rules

Building trust and innovative privacy solutions
United States

- **Blueprint** for protecting consumer data privacy and promoting innovation in the digital economy
  - Consumer bill of rights
  - Multistakeholder process to develop Codes of Conduct

- **FTC** takes a more active role
  - Report: Protecting Consumer Privacy in an Era of Rapid Change
  - Increased enforcement activity to protect consumer privacy

Building trust and innovative privacy solutions
United States

Main action items for the FTC:

- Do-Not-Track
- Mobile services
- Data brokers
- Large platform providers

Building trust and innovative privacy solutions
European Union

Draft Regulation for the protection of individuals and their personal data

➤ One law for the entire EU

<table>
<thead>
<tr>
<th>Strengthened Consent</th>
<th>Extraterritorial application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountability of processors</td>
<td>Significant penalties</td>
</tr>
<tr>
<td>Mandatory privacy officers</td>
<td>The right ‘to be forgotten’</td>
</tr>
<tr>
<td>Data breach notification</td>
<td>The right of ‘portability’</td>
</tr>
</tbody>
</table>

Building trust and innovative privacy solutions
Progress on Regulation so far:

- Multiple interests – companies (especially American), civil liberties proponents, data protection officials in the EU member states
- Amendments proposed by parliamentary committee (the Albrecht draft) in Jan 2013
- Voting on final Regulation not expected until late 2013
Cloud Computing

Building trust and innovative privacy solutions
What is cloud computing?

“[A] model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable resources (e.g., networks, servers, storage, applications and services)…”

National Institute of Standards and Technology (2011)

- On-demand service
- Resource pooling - scalable
- Measured service
- Rapid elasticity
- Broad and remote network access

Building trust and innovative privacy solutions
What is cloud computing?

- On-demand self-service
- Ubiquitous network access
- Location transparent resource pooling
- Rapid elasticity
- Measured service with pay per use

Building trust and innovative privacy solutions
Why some orgs engage CSPs

- Connecting with multiple devices, business agility and cost-cutting were the top three reasons cited for adopting cloud services (TNS)
- 88% of Australian organisations saw improvement in their IT departments since adoption of cloud (TNS)
- Australian public cloud market to reach $3.2 billion this year (Gartner)
Evernote says security breach by hackers

Online information storage firm Evernote has asked all users to reset their passwords, following a security breach by hackers.

The California-based company, that allows people to store and organise personal data on an external server, is thought to have about 50 million users.

It said user names, email addresses and encrypted passwords were accessed.

But it insisted there was "no evidence" that pay content was accessed, changed or lost.

Evernote acts like an online personal organisers: data such as video clips, images, web pages, or external storage system commonly known as IoT.

Building trust and innovative privacy solutions
Building trust and innovative privacy solutions
Preliminary privacy considerations

Types of data and privacy policies:

1. How sensitive or critical to your business is the data that the CSP will be processing/hosting?
2. Is the disclosure/transfer of personal information to the CSP authorised by your customers?
3. Whose privacy policy is the data subject to once outsourced – your business or the CSP’s privacy policy? Who owns the data once with the CSP?

Building trust and innovative privacy solutions
# Privacy risks

<table>
<thead>
<tr>
<th>Location and retention of data</th>
<th>Transferring data</th>
<th>Changing provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location of data and backups</td>
<td>Technical glitches</td>
<td>Unforeseen events</td>
</tr>
<tr>
<td>• Politically and environmentally stable regions?</td>
<td>• What happens when the data cannot be accessed or retrieved from the cloud service provider due to technical or other difficulties?</td>
<td>• What happens when CSP is shut down?</td>
</tr>
<tr>
<td>• Legal jurisdiction of data</td>
<td></td>
<td>• How is operational change handled - CSP bankrupt, sold, merged</td>
</tr>
<tr>
<td>• How does the CSP know where the data is?</td>
<td></td>
<td>• How is a disaster/hacking managed?</td>
</tr>
<tr>
<td>• With other clients’ data?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protection and Security</td>
<td>Protection and Security</td>
<td>Updates</td>
</tr>
<tr>
<td>• Encrypted whilst stored?</td>
<td>• Encrypted in transfer?</td>
<td>• Can upgrades to software or other services be refused?</td>
</tr>
<tr>
<td>• Who controls the encryption keys?</td>
<td>• Who controls the encryption keys?</td>
<td></td>
</tr>
<tr>
<td>• Physical security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retention</td>
<td>Subcontractors</td>
<td>Portability</td>
</tr>
<tr>
<td>• What are the data retention policies?</td>
<td>• Does the CSP use third party subcontractors?</td>
<td>• Can the data be easily relocated?</td>
</tr>
</tbody>
</table>
Among existing contracts for cloud-based services in Australia, many have problematic provisions:

- Not addressing access to or deletion of data, on service termination or breach of contract
- Limitation of liability for direct damages, exclusion of liability for indirect damages
- Unilateral variation of terms and conditions

Building trust and innovative privacy solutions
What’s in the contract?

- Onus on the customer to ensure privacy rules are complied with
- Onus on the customer to take security measures, with no mention of what would happen in the event of a security breach
- No control over third parties who receive the personal information in the course of providing the service

Building trust and innovative privacy solutions
# Model contract

<table>
<thead>
<tr>
<th>New Zealand Cloud Computing Code of Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate Identity</td>
</tr>
<tr>
<td>Ownership of Data</td>
</tr>
<tr>
<td>Security</td>
</tr>
<tr>
<td>Data Location/Geographic Diversity</td>
</tr>
<tr>
<td>Data Access and Use</td>
</tr>
<tr>
<td>Back up and Maintenance</td>
</tr>
</tbody>
</table>

Building trust and innovative privacy solutions
APPs and Cloud

- **APP 1**: current and clear policy about management of personal information, including disclosures to overseas recipients and their location
- **APP 5**: notice when personal information is collected, including if disclosed to overseas recipients and their location
- **APP 8 and section 16C**: in some circumstances may be liable for breach of APP by overseas recipient
- **APP 11**: destroy or de-identify personal information
# 10 Safeguards

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.</strong> Read the contract and terms of service very closely and clarify any ambiguous provisions</td>
<td><strong>6.</strong> Find out where and how the data will be kept</td>
</tr>
<tr>
<td><strong>2.</strong> Add cloud computing to your outsourcing and/or offshoring risk management frameworks</td>
<td><strong>7.</strong> Find out the CSP’s arrangements with subcontractors</td>
</tr>
<tr>
<td><strong>3.</strong> Ensure you are not violating any law or policy by putting personal information in the cloud</td>
<td><strong>8.</strong> Determine liability and accountability – what happens when things go wrong?</td>
</tr>
<tr>
<td><strong>4.</strong> Don’t put anything in the cloud that you wouldn’t want a competitor or government to see</td>
<td><strong>9.</strong> Have back-ups</td>
</tr>
<tr>
<td><strong>5.</strong> Clarify the rights of access, correction and deletion</td>
<td><strong>10.</strong> Establish your own security measures</td>
</tr>
</tbody>
</table>
Data Breaches

Building trust and innovative privacy solutions
Data breaches are pervasive

<table>
<thead>
<tr>
<th>RECORDS</th>
<th>DATE</th>
<th>ORGANIZATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>150,000,000</td>
<td>2012-03-17</td>
<td>Shanghai Roadway D&amp;B Marketing Services Co. Ltd</td>
</tr>
<tr>
<td>130,000,000</td>
<td>2009-01-20</td>
<td>Heartland Payment Systems, Tower Federal Credit Union, Beverly National Bank, North Middlesex Savings Bank, Golden Chick</td>
</tr>
<tr>
<td>94,000,000</td>
<td>2007-01-17</td>
<td>TJX Companies Inc.</td>
</tr>
<tr>
<td>90,000,000</td>
<td>1984-06-01</td>
<td>TRW, Sears Roebuck</td>
</tr>
<tr>
<td>77,000,000</td>
<td>2011-04-26</td>
<td>Sony Corporation</td>
</tr>
<tr>
<td>50,000,000</td>
<td>2008-08-27</td>
<td>Unknown Organization</td>
</tr>
<tr>
<td>40,000,000</td>
<td>2005-06-19</td>
<td>CardSystems, Visa, MasterCard, American Express</td>
</tr>
<tr>
<td>40,000,000</td>
<td>2011-12-26</td>
<td>Tianya</td>
</tr>
<tr>
<td>35,000,000</td>
<td>2011-11-10</td>
<td>Steam (Valve, Inc.)</td>
</tr>
</tbody>
</table>

Source: Largest Incidents: http://datalossdb.org/

Building trust and innovative privacy solutions
Impact of a data breach

- The average total cost per data breach in Australian organisations rose to $2.16 million in 2011
- Having a data breach caused by a third party mistake cost on average 35% more per compromised record
- Malicious and criminal attacks are the main cause and are also the most expensive, at $183 per record
- Organisations with external consulting support reduced cost of data breach by up to $45 per record

(2011 Cost of Data Breach Study: Australia, Ponemon Institute LLC (sponsor Symantec), March 2012)
# Causes of data breach

## Malicious or criminal attack (36%)
- Hackers or criminal insiders (employees, contractors, cloud providers, business partners) typically cause the data breach
- Viruses, malware, worms, trojans
- SQL injection
- Theft of data-bearing devices
- Social engineering

## Negligence (32%)
- Negligent employee or contractor
- IT and business process failures

## System glitch (32%)

(Based on data breaches experienced by 22 Australian companies within 10 industry sectors in 2011 – Cost of Data Breach Study: Australia, Ponemon Institute LLC (sponsor Symantec), March 2012)
Internal Threats

Reproduced with permission from Verizon: Based on Verizon 2012 Data Breach Investigations Report

Building trust and innovative privacy solutions
Data Breaches

1. How will you know if there is a data breach?

2. What happens when there is a data breach?

3. What resources exist to prevent and handle a data breach?

4. What data breach response plans are in place?

Building trust and innovative privacy solutions
1. How will you know if there is a data breach?

Reproduced with permission from Verizon: Based on Verizon 2012 Data Breach Investigations Report
2. What happens when there is a data breach?

Sony Data Breach Highlights Importance of Cloud Security

by Czaroma Roman on May 9, 2011 · 6 Comments

The Sony data breach that compromised millions of customers’ data has left the corporation a bit shaken and created woes for the cloud computing industry. The shares of businesses that specialize in cloud computing had been performing well for quite some time now. However, the massive cyber-attack, which left the company reeling, has put the brakes on plans of some companies to move their operations into the cloud. VMware Inc, which sells software for building clouds, experienced a 2 percent drop; Salesforce.com Inc, a maker of web-delivered software, has declined 3 percent.

Five lessons from the Distribute.IT hosting disaster

Wednesday, 22 June 2011 12:01

Patrick Stafford

The cyber-attack that crippled Melbourne-based web hosting provider Distribute.IT has left thousands of customers furious, with the data of almost 5,000 websites now deemed completely unrecoverable.

But the debacle has brought to light just how fickle the cloud can be. Combined with a security breach earlier this week from Dropbox and the massive cyber-attack against Sony, businesses everywhere are talking about cloud-based security.

Epsilon Data Breach Highlights Cloud-Computing Security Concerns

By: Fahimda Y. Rashid
2011-04-06

There are 0 user comments on this IT Security & Network Security News & Reviews story.

The theft of email addresses from Epsilon could affect consumer trust, and organizations have to reassess the risks of outsourcing less sensitive data and processes.

As email-marketing company Epsilon continues to deal with the fallout related to the revelation that some of its clients’ customer data has been exposed to a third-party, it becomes clear that this incident affects all service providers as organizations renew their focus on data security. In addition, this latest data breach calls into question how secure information is within a cloud-computing infrastructure.
3. What resources exist to prevent and handle a data breach?

- Steps you can take to minimise the likelihood of a data breach:
  - Privacy by design in business process and ICT
  - Privacy impact assessments
  - Privacy in risk management frameworks
  - Privacy skills development and training

- Check whether your insurer covers the cost of dealing with a data breach and notification

- Consider what your data breach response plan is
4. What data breach response plans are in place?

1. Contain the breach and do a preliminary assessment
2. Appoint lead person to manage (internal and/or external) response team
3. Evaluate the risks associated with the breach
4. Consider breach notification
5. Review the incident and take action to prevent future breaches

Building trust and innovative privacy solutions
Conclusion

- Data protection regulation increasing
- Privacy risks of cloud
- Safeguards
- Data breach is expensive
- How to respond to a data breach

Building trust and innovative privacy solutions
Further Information

- Cloud Computing in 2013 - What legal commitments can you expect from your provider? Shelston IP, March 2013

- Privacy and Cloud Computing for Australian Government Agencies, February 2013

- Draft Report on Cloud Service Provider Certification Requirements for the Australian Government, Department of Finance and Deregulation, December 2012
  http://agimo.gov.au/files/2012/12/csp-assurance-requirements-v0.5.pdf

- New Zealand Cloud Computing Code of Practice, Institute of IT Professionals New Zealand, June 2012

- Data breach notification - A guide to handling personal information security breaches, Office of the Australian Information Commissioner, April 2012

- Privacy in the Cloud: Key Questions, by Annelies Moens, Australian Corporate Lawyers Association, March 2012
  Vol 22, Issue 1

Building trust and innovative privacy solutions
Further Information

- 2011 Cost of Data Breach Study: Australia, Ponemon Institute LLC (sponsor Symantec), March 2012


Building trust and innovative privacy solutions
Questions?

Annelies Moens
Head of Sales and Operations
BSc, LLB (Hons), MBA

53 Balfour Street
Chippendale NSW 2008

Ph: +61 2 8303 2417
Au. M: +61 413 969 753
Int. M: +372 5437 1881
Fax: +61 2 9319 5754

amoens@iispartners.com
www.iispartners.com