Canadian report highlights US outsourcing dangers

A report published October 29th by the Privacy Commissioner for the Canadian province of British Columbia (BC) has raised serious concerns over the privacy implications of outsourcing public services to US-controlled companies.

The BC Commissioner, David Loukidelis, launched an investigation in early 2004 following concerns that the US Patriot Act (a piece of anti-terrorism legislation introduced post-September 11th) could be used to compel American-owned service providers to disclose private information on BC citizens.

The investigation solicited over 500 responses with the consensus of opinion concluding that US companies could be forced to "produce records held in Canada that are under the US corporation's control". As a result, public authorities or private sector companies outsourcing to US companies could be in breach of the BC Freedom of Information and Protection of Privacy (FOIPP) Act.

The BC government has been quick to act on these concerns and preempted the publication of the Commissioner's report by amending the FOIPP Act in early October. Loukidelis, however, has stated that the changes do not go far enough, and has made 16 recommendations for safeguarding citizens' privacy rights. The recommendations include:

• Amending legislation to prohibit the disclosure of personal data in response to a foreign court order or warrant - an offence that would be punishable by fines of up to CAN$1 million or a prison sentence.

• In order to uphold citizens' privacy, the BC government should establish a litigation policy that will allow it to initiate legal proceedings abroad.

• Carrying out immediate and comprehensive privacy audits of interprovincial, national and transnational public sector outsourcing agreements.

• Seeking assurances from US officials that they will not attempt to use the Patriot Act to access data on BC citizens.

• The introduction of legislative controls on information sharing and data mining.

Meanwhile, other countries are now starting to consider the implications of the US Patriot Act's disclosure powers on their own domestic privacy legislation. In November, the South Australian government announced that it would be looking into the activities of US-owned service providers after civil liberties groups raised concerns.

For the full report:: www.oipcbc.org

Bermuda plans privacy legislation

The government of Bermuda has announced plans to introduce new data protection legislation as early as next year. Speaking in London on November 16th, Michael Scott, Minster for Telecommunications and E-commerce, said that an initial draft bill has already been submitted to the Cabinet for review with a final version expected to be laid before Parliament in 2005.

Bermuda is fast becoming an important international business hub and a popular location for financial services organisations, and companies in the telecoms and e-commerce sectors. It is home to a $173 billion insurance industry and has attracted business from 75 per cent of Fortune 500 companies. With privacy becoming increasingly important in today's global information economy, the government has recognised the need to establish Bermuda as a secure and trustworthy place to conduct business through the implementation of effective regulation.

But while countries like India view data protection legislation mainly as a tool for encouraging offshore business, Michael Scott stressed that the protection of citizens' rights was an important incentive behind the proposals, adding that the new law would help to promote the growth in domestic e-commerce by raising the "confidence of Internet users in Bermuda". A government green paper published last year notes the importance of accurate data in the financial services sector, the privacy implications of workplace monitoring, and the commercial benefits that can arise from ethical privacy practices.

With regulation in Bermuda traditionally veering towards flexibility and pragmatism, Scott explained that the current draft is "drifting towards the American model" of privacy regulation as opposed to the stricter regime set out in the European Data Protection Directive. Although restrictions on data imports from the European Union pose obstacles for EU-based businesses with a presence in Bermuda, the government equally does not want to put off US business by imposing overly high standards.

Scott, however, added that the consultation "process is still very much open" and welcomed interested parties to come forward with their views.

The government has published a consultation document on proposals for data protection legislation. Comments can be sent to Kevin Anderson, Senior Analyst at the Ministry of Telecommunications and E-commerce. E-mail: kpanderson@gov.bm

EU backs ICC data transfer contracts

The European Commission is soon expected to give official backing to a new set of contractual clauses that will help businesses meet their legal requirements when transferring personal data outside the European Union. The new clauses were drawn up by the International Chamber of Commerce (ICC) and are seen as a more practical and business friendly alternative to the Commission's own contractual clauses, which have been the subject of much criticism from industry groups.

At an ICC meeting on October 26th, it was confirmed that the European Union's Article 31 committee (a data protection working group representing EU member state governments) had approved the ICC clauses. Although not yet officially approved, the Article 31 decision represents a major breakthrough and the Commission is expected to rubber stamp the decision as soon as December this year.

Robert Bond, Partner at Faegre Benson Hobson Audley and member of the ICC model clauses task force, believes the ICC approach will encourage more business to take the contractual route when transferring personal data outside the EU. "Because it has been drafted by business people for business people…it sits more comfortably with clients," he said.

In December last year, the situation looked bleak after a report from the Article 29 Data Protection Working Party (a group representing the EU data protection regulators) criticised the ICC clauses. According to Robert Bond, the ICC has since made some 'cosmetic' changes to the document which he believes helped to sway the Article 31 committee's decision.

For more information, visit the ICC website at www.iccwbo.org

European regulators rethink data protection strategy

The EU's Data Protection Working Party (a group of European data protection regulators) has outlined its approach to privacy regulation in a new strategy document. The Working Party - which produces guidance on their interpretation of the EU Data Protection Directive and advises the European Commission on data protection issues - has stressed the need to rethink its position following the growth in global data flows, the enlargement of the EU, and the advent of new regulations on electronic privacy.

One of the key issues outlined in the report is the number of divergences between EU data protection regimes, and the Working Party stresses that the need to improve harmonisation will be a priority over the next few months. The poor state of enforcement across Europe will also be tackled through a new sub-working group devoted to improving enforcement of national data protection laws. The Working Party reaffirmed its commitment to Binding Corporate Rules (a scheme that allows multinationals to manage privacy compliance through legally binding codes of conduct).

The Working Party has also addressed criticism over its 'closed shop' culture by pledging to be more proactive in its consultation with industry and by establishing communications channels with the media. And on the technology front, it has listed RFIDs, digital rights management and mobile location technologies as its focus for the short term.

See p.12 for an update on the European Commission's plans to improve data protection regulation.

ICC study offers hope for binding corporate rules

A study published by the International Chamber of Commerce (ICC) in October has concluded that despite a number of reservations, binding corporate rules (BCRs) can offer a viable and legal basis for data transfers outside the European Union.

BCRs essentially work by creating a 'safe haven' for customer and staff data within a multinational group, with affiliates being required to comply with an internal privacy code of conduct.

Many large organisations now see BCRs as a more business-friendly route to compliance than alternatives such as the European Commission's model contracts. However, European data protection authorities have yet to agree on the required criteria for approving pan-European BCRs and difficulties remain over how the schemes can be made legally binding.

The study shows that EU member states' legal systems differ in their approach to making these codes of conduct legally binding. To assess the variations, the ICC questioned 18 organisations from Europe, the US and Asia. According to the study, the "responses show that there is a wide variety of legal principles that may lead to legal enforceability of BCRs." The methods highlighted by the respondents include the use of a variety of contracts, or agreements involving unilateral declaration (although the study notes that not all jurisdictions will accept this approach).

See the full report at: www.iccwbo.org

Dutch regulator leaks e-mail addresses

The Dutch Data Protection Authority has found itself in the embarrassing position of violating the very law it is responsible for enforcing.

At the end of October, the regulator sent out a series of data protection e-newsletters to subscribers. But a technical error meant that one of the e-mails - sent out to a list of 1,000 people - exposed all the recipients' e-mail addresses. The situation was compounded when, after realising the mistake, staff at the Dutch DPA sent a second e-mail apologising for the error. Unfortunately, however, the same breach happened again.

According to reports, the e-mail list contained prominent data protection professionals, including the private e-mail address of Peter Hustinx, former Dutch Data Protection Commissioner and now the European DP Supervisor.

A spokesman for the Dutch DPA said, "Apparently, the list has become too long. We're looking into it to find a solution."

There have already been a number of similar incidents in which bulk e-mail communications have exposed recipients' personal data. In September, UK bank HFC exposed the e-mail addresses of 2,600 customers. The company was forced to apologise and pay out compensation (*PL&B UK*, Sept/October 2004, p1).

Cahoot admits online security breach

UK bank Cahoot was forced to shut down its website for 10 hours in October after being alerted to a security flaw enabling Internet users to gain unauthorised access to customer accounts. An investigation by the BBC revealed that the bank's password controls could be easily bypassed simply by typing in a customer's user ID.

Infosecurity expert, Neil Barratt, told the BBC, "I'm shocked that it was so easy", stressing that most online security breaches are generally more complex. One Cahoot customer described the breach as "disgraceful", adding that she would be closing down her account.

Tim Sawyer, head of Cahoot bank, a subsidiary of the Abbey National Group, said the flaw occurred as a result of an upgrade to the website. The flaw went by unnoticed for 12 days. Sawyer apologised, but attempted to reassure customers by stating that anyone hacking into the Cahoot site would not have been able to transfer funds out of the accounts. Sawyer stressed that the bank does carry out security testing on its systems, including penetration testing and the use of 'ethical hackers' to search for gaps in security. Nonetheless, he added that the incident had "not been our greatest moment" and pledged to conduct a review of security procedures.

Verizon wins battle over privacy and digital rights

On October 12th, the US Supreme Court upheld the right of Internet service provider Verizon to protect the identities of its customers. The Recording Industry Association of America (RIAA) launched a lawsuit in January 2001 after Verizon refused to comply with subpoenas that sought details on customers accused of illegally exchanging copyrighted music over the Internet.

Although losing the initial case, Verizon successfully argued before an appeal court in December 2003 that the RIAA's subpoena process - issued under the Digital Millennium Copyright Act (DMCA) - was unlawful. The Supreme Court's decision not to review the appeal court's decision has been hailed as victory for privacy and free speech by civil liberties groups, who have been concerned over the lack of judicial oversight in the subpoena process used by the RIAA. Wendy Seltzer, staff attorney for the Electronic Freedom Foundation said, "The DMCA doesn't give the RIAA a blank fishing license to issue subpoenas and invade Internet users' privacy."

Sarah Deutsch, vice president and associate general counsel for Verizon, said, "The Supreme Court has now finally shut a door that was otherwise left wide open to false accusations, negligent mistakes, as well as to identity thieves and stalkers, who could use the cursory subpoena process - without any judicial supervision - to obtain the name, address, and telephone number of any Internet user in the country - without the user even knowing about it."

In the next edition of PL&B International...

- Roundup on privacy notice requirements in Europe.
- Report from the EU Data Protection Working Party meeting on binding corporate rules.
- Could Australia's Anti-Spam Act be used as model for the rest of world?
- How data protection authorities handle consumer complaints.
- Latest developments on short privacy notices.