BNA International

World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Volume 9, Number 7 July 2009

Commentary

Databases: treasure or curse? In many ways databases are the backbone of our society. From client relationship management systems and lists of preferred customers, to health records or national databases of offenders they are seen as extremely useful tools allowing businesses and government to quickly access information that allows them to make decisions and coordinate their actions. Page 5

Amendments to the Indian Information Technology Act: implications for Australian corporations The Indian Government is in the process of finalising regulations to clarify the operation of various new provisions under the recent Information Technology (Amendment) Act 2008. Michael Pattison reports on the legislation, and on the implications for Australian corporations. Page 7

Administration proposes new Federal Consumer Financial Protection Agency Addressing the Obama Administration's proposals to reform financial regulation in the US, Barney Frank (D-MA), Chairman of the House Financial Services Committee, has promised to report legislation which would create a new Consumer Financial Protection Agency (CFPA) before the House adjourns for its August recess at the end of July 2009. Page 13

Privacy and social networking In June 2009 the Article 29 Data Protection Working Party, an independent European advisory body on data protection and privacy set up under Article 29 of Directive 95/46/EC ("WP-29"), rendered an opinion on privacy law implications of social networking ("WP-163"). In its WP-163, the WP-29 defines a social network service as "online communication platform which enable individuals to join or create networks of like-minded users" and categorises them as being information society services, as defined in Article 1 paragraph 2 of Directive 98/34/EC as amended by Directive 98/48/EC. The WP-163 stresses that the key phenomenon of social networks lies in the fact that users are asked to provide sufficient information about themselves in order to create a thorough personality profile or description and that moreover such information can be distributed to others. Page 25

News

Karen Curtis's tenure as Commissioner extended for another year Karen Curtis has been appointed for a further one year term as Federal Privacy Commissioner. Page 21

Article 29 Working Party releases opinion on social networking The Article 29 Working Party has released its opinion on social networking and how European data protection laws apply to social networking services. Page 22

Article 29 Working Party holds discussions with WADA The Article 29 Working Party held further discussions with representatives from the World Anti-Doping Agency (WADA) about the International Standard for the Protection of Privacy and Personal Information. Page 32

The Security versus Privacy paradox: a virulent fallacy under challenge

By Malcolm Crompton, Managing Director at Information Integrity Solutions [IIS].

How often have you heard somebody argue that there has to be a trade off between security and privacy?

The argument usually runs something along the lines that in order to keep you secure, you have to give up some aspect of your privacy. For example, you must exhibit a lot of evidence of identity before completing a transaction or joining a group or organisation.

This fallacy has been challenged vigorously many times with some of the most cogent reasoning coming from the Information and Privacy Commissioner of Ontario, Ann Cavoukian. She directly challenged the trade off concept in her 2002 paper "Security Technologies Enabling Privacy (STEPs): Time for a Paradigm Shift"[1] and followed up with "The Security-Privacy Paradox: Issues, Misconceptions and Strategies" in 2003[2]. The Commissioner first began drawing attention to the fallacy in 1995 in "Privacy-Enhancing Technologies: The Path to Anonymity"[3], a ground breaking paper published with her Dutch counterparts.

For all the effort that has gone into the challenge, the fallacy has lived on. But the tide is turning. On May 29, the US President released the 60-day Cyberspace Policy Review.[4] Item 10 in the Near Term Action Plan put forward by the review calls for the nation to:

"Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation."

Read the US President's remarks at the time of the release[5] and count how many times he remarks on the importance of getting privacy AND security right.

Why is this relevant to such campaigns as National E-Security Awareness Week which took place in Australia in June?[6]

Because if nothing else, the two concepts do inform each other. Here is an example: it is possible to improve the security settings in your organisation by intelligently applying privacy principles such as those seen in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[7], the APEC Privacy Framework[8] and many laws worldwide. For example, consider the National Privacy Principles (NPPs)[9] in the Privacy Act of Australia[10]. In particular, consider the security guidance supplied by the following NPPs:

NPP1, The Collection Principle: "An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities." From a security perspective, the less personal information you collect, the less there is to keep secure and the less to lose. And the less attractive your data sets are to those who want to steal it. An additional bonus: this should also reduce your data handling costs.

NPP2, The Use and Disclosure Principle: "An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless" certain limited exceptions apply. This is totally in line with the 'need to know' adage in any security framework.

NPP3, The Data Quality Principle: "An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date." One of the most significant weaknesses in any organisation's security framework is its ability to ensure not only that new staff and contractors are properly provisioned with resources when they commence, but are also DE-provisioned when they leave.

NPP4, The Data Security Principle: "An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure." and "An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed. . ." Enough said!

And so it is possible to work your way through the NPPs in this way.

But in a sense, that is old news. Take emerging technologies and business processes such as the urge to make more use of cloud computing than is already happening with search, data storage, email etc. The perspective in "It's 6 O'Clock - Do You Know Where Your Cloud's Data Center Is?"[11] that was carried in Information Week on June 2, 2009 is well worth reading.

Even if all this guidance is applied well, data losses will happen even in the best run organisation. What to do then? Again, it is possible to plan a response based on the hard-learned lessons of recent years from the losses of personal information.

Malcolm Crompton can be contacted at: MCrompton@iispartners.com. IIS is a specialist privacy consultancy; its services include privacy impact assessments, privacy thought leadership and advice and strategy. Information about IIS is available at www.iispartners.com. Malcolm regularly blogs on www.Openforum.com.au. An earlier version of this article first appeared on the Open Forum.

  WDPR ISSN 1473-3579

The 2009 Data Breach Investigations Report[12] , a study conducted by the Verizon Business RISK Team provides plenty of surprising insights as to where the security weaknesses in many organisations might really be. The Office of the Privacy Commissioner of Australia has also published a "Guide to handling personal information security breaches".[13] At IIS, we have published a Privacy Breach Check List.[14] The check list provides immediate help in the first 24 hours of a major data loss and suggests what to do as matters unfold over the first week and what to think about in the longer term.

In short, Security AND Privacy go hand in hand, neither by itself sufficient, both informing the other.

And the discussion will continue. The 31st International Conference of Data Protection and Privacy will be held in Madrid in November.[15] Like many of its predecessors, it will be supported by a number of very challenging preconferences. One will be *Privacy by Design: The Definitive Workshop*, which will be held on Monday, November 2 2009 at the Hotel Melia Castilla in Madrid. Participants will hear from a global cross-section of privacy leaders who will describe their real-life experiences and plans for the use of Privacy by Design. Participants and speakers will include Ann Cavoukian, the Privacy Commissioner of Ontario, Canada, Yoram Hacohen, Head of Israeli Law, Information and Technology Authority, Peter Hustinx, the European Data Protection Supervisor, Dr. Jacques Bus, Head of Unit for Trust and Security in ICT Research at the European Commission, Dr. Alexander Dix, Data Protection and Freedom of Information Commissioner for Berlin, Germany and the Honourable Pamela Jones Harbour, US Federal Trade Commissioner.

The fallacy may continue, but there is a good chance it will be seen in more realistic light soon.

NOTES

1 http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=245

2 http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=248

3 http://www.ipc.on.ca/images/Resources/anoni-v2.pdf

4 http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

5 http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/

6 http://www.business.gov.au/Business+Entry+Point/News/National+Esecurity+Awareness+Week.htm

7 http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_119820_1_1_1,00.html

8 http://www.apec.org/apec/news___media/2005_media_releases/161105_kor_minsapproveapecprivacyframewrk.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1

9 http://www.privacy.gov.au/publications/npps01.html

10 http://www.comlaw.gov.au/comlaw/management.nsf/lookupindexpagesbyid/IP200401860

11 http://www.informationweek.com/cloud-computing/blog/archives/2009/06/its_6_oclock_do.html

12 http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

13 http://www.privacy.gov.au/publications/index.html#G

14 http://www.iispartners.com/downloads/2006-07-Security-breach-checklist.pdf

15 http://www.privacyconference2009.org

News

ASIA PACIFIC

Highlights from the 31st APPA meeting

The Asia Pacific Privacy Authorities held their 31st Forum in Hong Kong, June 11–12, 2009.

APPA members reported on national and international developments, in particular, there were discussions about how to deal with the privacy challenges surrounding new technologies and the security issues posed by portable storage devices. The Working Group for Privacy Awareness Week also reported on the success of the 2009 Privacy Awareness Week held in May. It was agreed that the Privacy Awareness Week for 2010 will also take place during the first week of May.

Other topics discussed included data breach notification developments in Asia Pacific and an update on the APEC Privacy Framework. Discussions were also held about how best to deal with the privacy implications of electronic health records.

The 32nd APPA meeting will be held during the first week in December, 2009 in Adelaide, Australia.

For more information about the outcomes from the Forum, visit:

http://www.privacy.gov.au/international/appa/hongkong-communique.html

AUSTRALIA

Karen Curtis's tenure as Commissioner extended for another year

Karen Curtis has been appointed for a further one year term as Federal Privacy Commissioner. Her term has been extended so she can oversee the transition period where her Office assumes responsibility for Freedom of Information and Privacy to become the Office of the Information Commissioner (OIC).

The OIC will include two new posts; an Information Commissioner and a separate Freedom of Information Commissioner. The Australian government has allocated AUS$20.5 million over a four year period to establish the new information agency. Karen Curtis's one year term starts from July 12, 2009.