Australian businesses consider a role for risk ratings in new thinking on privacy and trust

By Malcolm Crompton, Chris Cowper, and Martin Abrams

The Privacy and Trust Partnership (P&TP), a consortium of Australian businesses which included a credit reporting bureau, data brokers and IT companies and whose core activities rely on the use of personal information, last year sponsored a project to consider privacy protection and trust in the information economy.

Malcolm Crompton

Chris Cowper

Martin Abrams

The consortium's view was that the traditional approaches to protecting individual privacy—based on 30-year-old thinking—are struggling to keep pace with the realities of the speed and volume of the flow of personal information in the world's economies, let alone new uses such as business analytics. These approaches are embodied, for example, in early credit reporting law, Fair Information Privacy principles, and the 1980 Organisation for Economic Co-operation and Development (OECD) Guidelines on Transborder data flows.

The aim of the P&TP project was to find a better approach, recognizing that more innovative thinking would be required than is often applied. The payoff would lie in safely unlocking the further enormous potential value in personal information in a way that all parties would appreciate and find trustworthy.

About the project

There were two components to the way the P&TP project was undertaken. Firstly, it was recognized that to be effective, any new approach to privacy and trust would need to consider the interests and values of all of the players. To this end the consortium hosted two workshops bringing together key Australian stakeholders in the personal information use debate, including businesses, consumer and privacy advocates, and regulators.

Secondly, the consortium sought some innovative thinking from Information Integrity Solutions Pty Ltd (IIS), and the Centre for Information Policy Leadership (CIPL) prepared two papers: A New Approach to Trust and Privacy in the Information Age; and a working paper which proposed some themes and a possible framework based on a privacy risk rating. The papers and other information about the project are available at www.iispartners.com and www.openforum.com.au/Privacy_and_Trust.

Scoping the problem

The P&TP papers explored the proposition that there is enormous value to be unlocked for everybody in the responsible use of personal information, often found in ways not previously anticipated. Alan Greenspan, for example, pointed to its value in terms of reducing "knowledge float" because it is a valuable input to data analytics for risk management, marketing etc, in online transactions or in new or improved business processes (transcript found at www.federalreserve.gov/BoardDocs/Speeches/2000/20000414.htm).

The papers argued that this potential is clouded by a worrying conundrum: despite an increasing array of laws designed to protect personal information and security, nobody is fully satisfied with the result. Individuals do not feel that their personal information is safe, businesses find privacy rules constraining and onerous, and government officials and regulators find it difficult to respond effectively to the needs of either group. In short, current and future uses of personal information and personal safety are at risk. This situation appears to be true across economies, whether in Australia, which has a general privacy law as well as specific issue laws, or the United States, which to date has dealt with issues sector by sector (credit reporting, Gramm Leach Bliley, HIPAA, Do-Not-Call, etc…) or elsewhere.

The consultants pointed to a range of contributing factors including:

- the almost unimaginable amount of personal information generated in the digital economy; one article puts it at "three million times the information in all the books ever written," with predictions that by 2010 the volume will increase "more than sixfold to 988 exabytes." ("Humans Created 161 Exabytes of Data in 2006," iTnews.com.au, March 7, 2007, www.itnews.com.au/print.aspx?CIID=74870&SIID=35.);

- traditional privacy principles rely on giving individuals fine-grained control via notice and consent mechanisms which, together with the inherent purpose limitations, adds up to a costly, inflexible regime for business, which is also stifling to innovation;

See, ***Australian risk ratings,*** *page 10*

Australian risk ratings

continued from page 8

- the current rules rely on individuals being able to make rational choices and being the front line enforcer of their own privacy when things go wrong. In practice, the result for individuals is too many notices and too little time and expertise to assess them or enforce their decisions;

- such privacy rules also tend to assume binary relationships between individuals' and business, not the networking of information and extended value chains that characterise both the online world and current business models (analytics, Facebook, credit reporting, ID authentication, data cleansing, outsourcing ...)

- the absence of individual comfort and disconnects between business and individuals' expectations means that the law tends to develop haphazardly as particular issues become an 'emergency' concern—for example, do-not-call registers in the United States and Australia and the various United States data breach laws (which may soon come to Australia).

Some possible themes for a new privacy and trust framework

A number of themes and ideas emerged from the P&TP papers and workshops that seem likely to bear fruit if used to guide development of new privacy frameworks. These include that:

- the emphasis should be on outcomes rather than processes—what will success look like rather than outlining requirements to give notice, for example;

"There must be a fair allocation of risk, control for individuals, and accountability leading to an environment of trust."

- individuals should have sufficient control, or be confident that information is under control, and feel that they are getting value and are safe regardless of how freely the information moves;

- businesses need predictability and freedom to innovate;

- there must be a fair allocation of risk, control for individuals, and accountability leading to an environment of trust;

- rules, standards or principles are needed to establish a common language and expectations around the framework, and these need to be kept flexible and adaptable, and to line up with other information governance frameworks, such as for financial information; and,

- an effective framework will need to include enforcement mechanisms. "Responsive regulation" was suggested as guide to striking a balance between assistance, inducements, and punishments, with the emphasis on the former (see the writings of Professor John Braithwaite at www.anu.edu.au/fellows/jbraithwaite/).

Other ideas explored included the management of personal information by "trusted agents," clearer answers to "who bears the risk" in transactions, and insights from other regulatory models, for example, environmental protection where the "polluter pays" in order to internalise economic externalities.

Privacy risk rating to calibrate business privacy obligations

The second P&TP paper attempts to draw these themes and ideas into a framework. The model is based on a binding privacy framework approach (BPF)—similar to the Australian notion of approved privacy codes or the EU notion of binding corporate rules—that would cover not only "privacy principles," but also the accompanying compliance framework and the notion of a privacy risk rating.

The BPF and the risk rating would combine as levers to increase the stakes to the extent that organisations internalise the need for privacy action, for example, in relation to what personal information is collected, or how privacy risks are managed. In return organisations get greater flexibility in managing their obligations, greater assurance that their actions will be "trusted" as individuals become confident that the systems work without them needing to police their privacy, and the freedom to innovate both in business processes and in use of personal information.

"There is indeed a range of perspectives and strongly held views that will be brought to bear on this issue."

The paper suggests that the privacy risk rating system would aim to inform and mobilise market forces and would be backed by an enforcement regime to reinforce the benefits of lowering the rating to a business. The rating, for example, would be designed to influence consumer choice and influence costs of capital, both providing an incentive to seek a more privacy respecting rating. Components of the enforcement regime that could be made dependent on the rating, in order to reinforce even further the incentive to improve privacy practices, could include the assurance or external accountability obligations and level of penalties to which the organisation is subjected.

In developing the model, further choices would have to be made at a number of levels. For example: would the rating be voluntary or mandatory, would the risk rating be established in law or set by an independent body which would undertake the rating process, and what factors would determine risk rating?

In conclusion

The P&TP discussions have confirmed that there is indeed a range of perspectives and strongly held views that will be brought to bear on this issue. The discussion to date has been robust, and the next step in the process

will be to look at all the ideas that have come forward and to see which should be developed. The one thing we can be sure of, though: doing nothing is not a viable option.

Malcolm Crompton *is managing director of Information Integrity Solutions P/L, advising private and public sector organisations on building trust through the way they collect and use personal information. He was Australia's Privacy Commissioner for five years until April 2004. He is also a member of the Board of the International Association of Privacy Professionals. www.iispartners.com*

Chris Cowper *is a principal consultant with Information Integrity Solutions P/L. Her recent projects have included privacy impact or risk assessments in the education and resource sectors, privacy training in the health sector and thought leadership on privacy regulation. Before joining IIS in 2007, Chris spent 16 years with the Office of the Australian Privacy Commissioner. www.iispartners.com*

Martin Abrams *is executive director of the Centre for Information Policy Leadership at Hunton & Williams LLP. He has been an innovator in information, privacy and security for nearly 20 years, helping to shape digital-age global privacy concepts by providing thought leadership for companies, consumer leaders, and policy makers.*

Hear more from ***Malcolm Crompton*** *in his "Top 10 Requests for EU Directive Review" session at next month's Privacy Summit in Washington, DC. www.privacysummit.org*

Hear more from ***Martin Abrams*** *at his "It's Time for a New Privacy Framework in the U.S. and Globally" session.*

knowledge net

Lofty lesson on breach notification

From the 47th floor of Boston's John Hancock Tower on a clear autumn day, you can see a lot. There are the long rows of brownstones, the Zakim bridge, Frank Gehry's wonderfully crooked Stata Center across the Charles River at MIT, and Fenway Park, in all its post-season glory, on the day of game three of the American League East 2008 playoffs.

It's a long view to be sure, but there's no glimpse of the future. Not even from New England's tallest building. So on an October morning, as Red Sox Nation awoke anticipating the outcome of the evening's game, IAPP members eager to get a leg up on compliance with the Massachusetts data breach notification law gathered in a board room at Ernst & Young's Hancock headquarters to hear from Scott Schafer.

Schafer is deputy division chief in the Consumer Protection Division at the Office of Attorney General Martha Coakley. He's the guy who, for one, fields notification letters from Massachusetts entities that experience a data breach.

The Massachusetts law requiring breach notifications went into effect in October 2007, but at the time of this event, no enforcement actions had taken place. Schafer said for the past year his office has focused on educating entities on the ins and outs of the law, and will shift to more of an enforcement focus in the coming months.

"Other states are looking to Massachusetts because our regulations have a higher standard," said Schafer, who has been a victim of data-breach induced identity theft.

While attendees munched on a hot breakfast, Schafer gave the 600-foot view on becoming compliant, and fielded questions from the audience.

"Massachusetts may be late to the game as far as adopting data breach notification legislation," said Mike Spinney, CIPP, principal of SixWeight and IAPP co-chair for the event. "But the state's new law has a number of unique provisions that attendees were eager to learn more about."

And Red Sox Nation? Let's just say they were less eager to hear the outcome of game three.

For a schedule of all upcoming KnowledgeNet events, visit www.privacyassociation.org and click on "Network."

Scott Schafer, deputy division chief in the Consumer Protection Division of the Massachusetts' Attorney General's Office addresses IAPP members in Boston.