HOW HAS THE PRIVATE SECTOR REACTED TO THE PRIVACY ACT—A PRACTITIONER'S PERSPECTIVE?

Michelle Narracott*

Paper presented at the ANU Public Law Weekend, Canberra, 2 November 2002

Introduction

It is almost 12 months since the Federal Privacy Act 1988 was extended to private sector organisations with a turnover of $3 million or more[1], as phase one of the privacy implementation within the private sector. At that time, the Federal Privacy Commissioner, as regulator was given jurisdiction to monitor, guide and penalise those businesses failing to meet the 10 National Privacy Principles (NPPs).

In my view, since 21 December 2001, the Privacy Commission and the private sector have engaged in one of the more productive regulatory relationships Australia has experienced in recent years. Although largely over-shadowed both in the media and the boardroom as an item of major note by more fundamental corporate governance issues striking at the core of companies' survival, the privacy rollout and the call for compliance to Australian businesses has proceeded smoothly, without exception.

It has been said that good news does not make for interesting press. Despite this risk, this paper makes no apologies for sharing a good news story about the Federal Privacy Commissioner's approach to facilitating privacy compliance within Australia's private sector and the private sector's response. However, my final message is a challenging one. At this point, we do not know whether privacy has been implemented effectively within the private sector. From the ground, there are signs of difficulties in embedding compliance programs.

This paper gathers my perspectives, as a corporate governance practitioner, adviser and reviewer/auditor of privacy compliance programs, of the first year of the operation of the Privacy Act in the private sector, and highlights trends and challenges. Three key areas of observations are addressed:

1 The response of Australian business to the call for action on privacy reform.

2 The actions and response of the regulator, the Federal Privacy Commissioner, in moving the private sector towards compliance.

3 Meeting the challenge of successful privacy implementation.

---

* *Partner, Deloitte Touche Tomatsu.*

The Response of Australian Business – setting the context

Pre-21 December 2002 concerns

During the early part of 2001, the media and some industry organisations developed an increasingly worrying picture about the demands which would be placed on business in meeting the Privacy Act start date of 21 December 2001. This scenario was supported by the Chartered Secretaries Australia (CSA) survey results[2] of Company Secretaries in the Top 200 companies conducted in May 2001 (Survey No 3). The survey highlighted a significant concern that 42.3 per cent of respondents believed that they did not have sufficient time to prepare for the new obligations under the Privacy Act.[3] However, by November 2001, many business advisers and industry organisations were acknowledging what the Privacy Commissioner had been pledging, that the Commissioner would be taking an educative, facilitative approach in the first year of the Act's operation in the private sector.[4] With Christmas looming, there was a collective sigh of relief.

For the 12 months leading up to 21 December 2001, the Privacy Commissioner had adopted a range of measures to involve affected businesses and prepare for the rollout of privacy laws. This included the 'open letter' approach in which the Commissioner sought assistance with, and feedback on, guidelines to clarify the NPPs, and on guidelines for organisations and industries wishing to develop their own approved code to replace the NPPs. Suggestions and comments were sought on the type of information and assistance which businesses would find most useful as they prepared for the commencement of the Act.

The private sector was also flooded with a plethora of self-help privacy toolkits and a range of privacy health checks from industry bodies, the consulting sector and law firms. In the main, the products on offer were remarkably standard in nature featuring step by step instruction on determining the application of the Privacy Act, analyses of personal information use, assessing privacy exposures and developing privacy compliance policies, statements and programs. The Australian/New Zealand Standard on Compliance AS/NZS 3806: 1998 has formed the basis of many of the products and approaches on offer. Despite these offerings, in the main private sector organisations were to take a low key, in house approach to preparing for the privacy implementation.

Getting privacy on to the agenda: Yet another legal compliance issue

One of the challenges for the Privacy Commission has been managing business' view that privacy is just another compliance issue to be added to the already overflowing in-trays of Australian compliance officers. Another compliance issue to compete for the officer's time – to be absorbed, developed into organisational policy, pushed through the Board approval and a compliance manual/implementation program created.

The reality is that adherence to the requirements of the Privacy Act is yet another matter of legal compliance for business. Privacy obligations are placed on company legal compliance registers by company secretaries, along with the list of other legislative requirements the business must meet, and as time allows, addressed according to well-established management discipline and principles for ensuring that organisations 'get it right' in relation to their legal obligations. However, we are observing a subtle change. Although we continue to encounter this minimalist approach to privacy control, 18 months ago it pervaded. What has changed? We are now in a time of unprecedented focus on corporate governance, legal and regulatory issues. Boards and audit committee members are feeling their immediate fiduciary and shareholder confidence pressures, and are more motivated to tackle governance issues, than at any time since the corporate collapses of the 80s.

Over the past three months, Deloitte's experience is that compliance issues including privacy are being given far more attention in the boardrooms of Australian companies than ever before. Best practice management and treatment of legal and business exposures and ensuring the processes are in place to deal with the risks are being brought forward on board and audit committee agenda across the country. This augurs well for successful privacy implementation.

These observations are fully consistent with the findings of a recent survey[5] targeting Australia's top-500 listed companies by revenue with the largest group of respondents coming from organisations of more than 100 employees. The survey indicated that 96 per cent of the directors and 92 per cent of senior management were strongly committed to implementing legal compliance. Some 91 per cent have appointed a compliance manager and all organisations surveyed had identified the key laws relevant to their business activities.

The Features of the Private Sector's Response

What then have been the key features of the private sector's response?

A smooth and uneventful transition.

Despite the many gloomy predictions during 2001, my on-the-ground observation is that the private sector transition to the new privacy law reform implemented on December 21, 2001 has been remarkably smooth and uneventful.

The CSA survey results[6] of Company Secretaries in the Top 200 companies' compliance pre- and post-law reform reflect a similar sentiment. The surveys conducted in May 2001 and February 2002 indicated widespread acceptance of the need for privacy regulation in the private sector and the broadly-held view that the change process has not been burdensome in its initial requirements, nor in its implementation (92 per cent of respondents).

Post-implementation of the Act, the need for some finetuning of the Act was identified by 69 per cent of respondents, which CSA further specifies as including greater clarification of penalties for non-compliance and clearer explanations of principles.

In conclusion, 88 per cent of respondents in the post-Privacy Act survey indicated that they were not experiencing any difficulties in complying with the Act. Some 92 per cent indicating that ongoing compliance with the Act was not seen to place an unnecessary burden on companies.

Table: Chartered Secretaries Australia: post Privacy Law Reform Survey Results

Now that the Privacy Act has come into effect, do you believe there was sufficient time To prepare your Company's database of clients/customers for the new obligations under the Act?	
Yes = 77%	No = 23%
Are you experiencing any difficulties in complying with the Act?	
Yes = 12%	No = 88%
In your view does the Act require fine tuning?	
Yes = 31%	No = 69%

Did your organisation implement the Act by adhering to the National Privacy Principles (NPP) in the Act or did your organisation develop it's own privacy codes?		
NPP = 88%	Own 12%	
Did your company appoint the Company Secretary as the Privacy Officer?		
Company Secretary = 62%	Compliance Officer = 15%	Other = 23%
Do you believe that ongoing compliance with the Act will place an unnecessary burden on your company?		
Yes = 8%	No = 92%	

Heightened awareness that consumers take the issue seriously

Through Privacy Commissioner media releases, media reports and their own consumer feedback, business is aware that privacy is important. Since 21 December 2002, the Privacy Commissioner has reported a three-fold increase in calls to the Office and a four-fold increase in written complaints to the Office. During the first six months of the new Act's operations, the Office of Federal Privacy Commissioner (OFPC) received more calls to the hotline (13,450 calls in total) than for all of 2001 (8,177 calls in total). Written complaints to the OFPC also rose with 456 written complaints lodged in the first six months, compared to 194 written complaints lodged during all of 2001.[7]

The key issues reported by the OFPC as of concern by consumers include:

- inappropriate disclosure of information;
- accessing information;
- being pressured into consenting to many uses of information in order to receive a good or service from an organisation (bundled consents);
- direct marketing continuing after asking an organisation not to make contact; and
- unnecessary collection of information.

Business opting in

Section 6EA of the Privacy Act allows private sector organisations who would not otherwise be covered by the Act to elect to be treated as an organisation for the purposes of the Act. This includes being exposed to random audit and investigation by the Privacy Commissioner. The potential attraction of the provision is that small businesses may be able to generate increased consumer confidence and trust if they are able to demonstrate to their clients and customers that they are subject to, and abide by, the NPPs and operate under the Privacy Act.

A public register of businesses who have elected to 'opt-in' is available on the OFPC website. To date, some 75 small businesses have opted-in with the majority of businesses represented being community, employee and cooperative credit units and consulting organisations.

Development of industry codes

The Privacy Act allows organisations and industries to have and to enforce their own privacy codes that continue to uphold the privacy rights of individuals while allowing some flexibility of application for organisations. Under section 18BB the Commissioner may approve a privacy code, provided certain criteria are met.

Numerous private sector codes have been developed as at 1 November 2002, including the General Insurance Information Privacy Code and the Clubs Queensland Industry Privacy Code. Several codes are under development, eg the Market and Social Research Privacy Code and Australian Casino Association Privacy Code.

Incorporating privacy into corporate risk management and internal audit programs

More progressive boards and audit committees have identified privacy compliance as a corporate risk and have incorporated privacy as an exposure within the company's corporate risk management program. Unlike the public sector where corporate risk management programs are now well established – some 70 per cent of agencies within the Commonwealth have commenced corporate risk programs – the private sector is just starting to establish programs for systematically identifying risk.[8]

By taking a risk-based approach to managing privacy obligations, privacy risks can be identified, assessed, prioritised and then treated through removal of the risk or mitigation, in an ordered and auditable manner. Privacy controls can be established which are designed to address the real risks associated with personal information management within the business.

In the profession's experience, some but not sufficient, companies have placed or plan to place privacy onto the internal audit program to ensure that the controls for managing privacy issues are effective and implemented. As part of the audit program, the company's internal auditors with the cooperation of corporate and line management conduct a privacy review or audit regularly. The audit program has the benefit of preparing the company for random audits by the Privacy Commissioner.

Balancing the regulator's role – Getting the approach right

Administrator v Watchdog?

The Federal Privacy Commissioner, Malcolm Crompton, has maintained (without appearing to waver) the moderate and reasonable regulator approach. Quoted many times [9] as stating that his approach is to help business to comply with the Act, our observation is that Crompton has demonstrated that this is not purely rhetoric. One of the new regime's more scathing commentators, Dr Robert Clarke, was reported as criticising the Privacy Commissioner in the prelude to 21 December 2001 for being an administrator when he needed to be a watchdog.[10] The Privacy Commissioner has made no apologies about his more facilitative approach. This approach is fully consistent with the best practice messages used for achieving the necessary levels of legal compliance motivation.[11]

The five key messages going to Australian business from the OFPC are clear and persuasive. In summary, the messages read:

Pride – Highlighting the business' reputation for integrity and the benefits that will flow. Good privacy is good business and compliant privacy practices will build positive relationships with customers whilst meeting responsibilities under the Act.

Up to date – Managing privacy fits in with the business' focus on progress and governance reform.

Active rather than passive – Emphasising advantages in taking the initiative in privacy control rather than waiting for an incident to occur.

Piece of cake – Privacy control is not complex and requires modest outlay.

Over a barrel – If all else fails, privacy control is a compliance requirement.

Setting the tone for handling transgressions – the Transurban Response

Earlier this year, the private sector watched the OFPC's handling of the Transurban case as somewhat of a test of whether the Privacy Commissioner's actions would be consistent with his published approach. In the case of Transurban, an ex-employee had disclosed thousands of customer credit card numbers over the internet. The OFPC conducted a review of Transurban's information handling practices, as a result of the disclosure. The review found that Transurban needed to address certain areas to reduce the overall risk of further privacy breaches. An independent review at the time also found Transurban had 'best practice' data security consistent with the nature of the information held.

In a press release, the Privacy Commissioner publicly commended Transurban for its promptness and decisiveness at the time of the breach. The actions taken by Transurban included the issue of a press release immediately following the incident and publication in the Melbourne press of an open letter apologising to customers and informing them of its intended actions.

The challenges and shortcomings of the private sector's response

It is only 10 months since the Privacy Act commenced its operation within the private sector. As this paper has highlighted, the indications are that the basis for a healthy regulatory relationship has developed between the private sector and the Federal Privacy Commissioner. However, these are the earliest days of a major private sector implementation program for the Federal Government. The real challenge for both regulated and regulator is to ensure that the privacy management and controls put in place over the past year are effective and are actually embedded into the everyday operations of Australian business. There are some hurdles to overcome before we can conclude that the private sector response has been sufficient.

Window dressing or substantial implementation?

Have the private sector organisations put in place effective privacy programs? At this point, there is limited evidence available from the OFPS or from the private sector itself from which to draw any significant conclusions. Privacy policies, statements and consent notices on websites, in marketing materials and business forms have become common place as public indicia of business' compliance with privacy obligations.

In the absence of any data of significance, some practical insights and general observations as a practitioner may be of value. At this time of year, internal audit programs are well underway in most private sector organisations. Tasked by boards and audit committees to provide assurance about the levels of compliance, privacy audits should now be standard items on Australian company audit programs, in preparation for potential external monitoring of compliance and for the purposes of providing feedback on the effectiveness of the internal privacy program. My concern is that privacy audits are not to be commonly found on audit programs. The challenge for the private sector is to correct this.

In Australia, audit functions have been slow to respond to a world-wide call to add value in relation to non-financial performance as well as financial performance. Privacy compliance, as a non-financial performance item, is often overlooked. Privacy is marginalised as a compliance issue in some organisations. Management of the issue has been given to Legal, Human Resources or Information Technology functions. Although skilled in the technical issues of their disciplines, our experience is that direct knowledge of risk management, internal control and compliance methodologies and processes is often lacking with the result

that the strength of the program is often corporately inconsistent, less rigorously pursued and less effective than it would be if it was considered a mainstream compliance issue.

Many private sector organisations (and public sector organisations!) have significant gaps between the way they currently control their business to manage their compliance exposures and established best practice.[12]

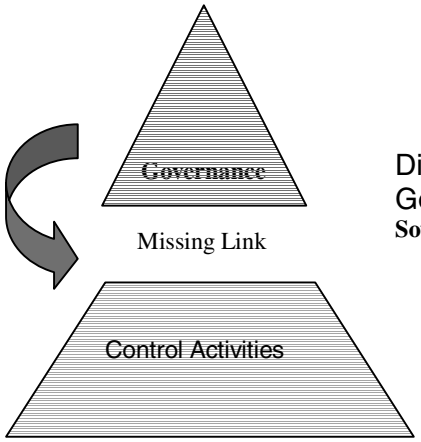

Diagram: The Missing Link – Linking Governance & Control
Source: Deloitte Touche Tohmatsu

In Australia and globally, companies are struggling with the following four vital elements of effective compliance:

1 **Risk assessment**: Developing responses to compliance issues, which are risk-based. This means first determining the risks and exposures arising from the management of personal information.

2 **Control Activities** – Good risk mitigations and control: Once the risks are identified, then determining the most appropriate mitigation strategies or internal controls.

3 **Monitoring** – Program Regularly updated: Ensuring the risk assessment is revised and still current, and regularly monitoring the controls and their usage through regular audits to determine whether they are still effective in minimizing the potential for breach of privacy obligations.

4 **Information and Dialogue**: Board, audit committee, staff and clients educated about the controls and monitoring process to ensure understanding, and necessary motivation to implement.

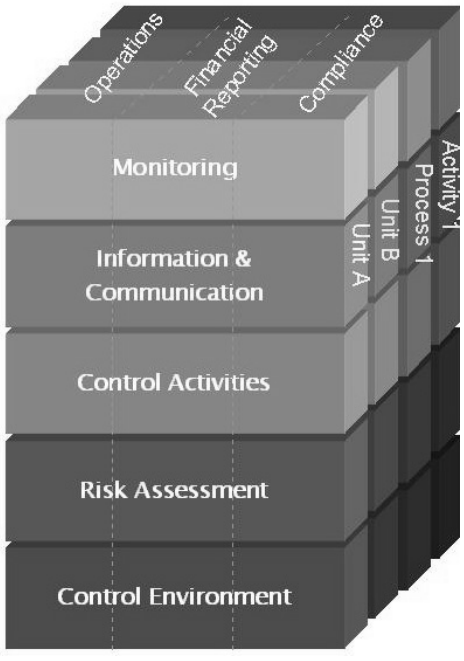

Diagram: The elements of a best practice control infrastructure – Source: Deloitte Touche Tohmatsu

A recently released survey [13] confirms what the internal audit and consulting profession is encountering anecdotally every day. The National Compliance Survey conducted by Ernst and Young of the top 500 companies listed on the Australian Stock Exchange identified a major gap between the committed stance taken by board members and senior management in operating a compliant company and the actions of the company in managing for compliance.

The Ernst and Young survey revealed a significant disparity between the Board's intentions and the reality of day-to-day operations. In some 42 per cent of respondents, compliance is not yet considered a standard part of business practices. In the highly regulated financial services sector, where compliance is paramount for business licensing purposes, 34 per cent of respondents did not see compliance as a core business function.

69 per cent of respondents had undertaken a risk assessment of their compliance obligations and identified higher priority legal requirements. Of these organisations, only 71 per cent had developed written processes to enable staff to manage these risks. More telling was that only 19 per cent saw 'communicating expected behaviours to staff' as a key objective of a compliance program.

Likely impact of CLERP 9 and Sarbanes-Oxley

The Treasurer's recently announced corporate governance reform package has major potential to improve Australian company management of privacy and other compliance obligations. Specifically, a number of the reform proposals focus on the need for the Board to ensure it is receiving adequate information and assurance from management about the processes the company has in place for managing legal obligations and risk exposures. The responsibility for this has been placed firmly with Board audit committees in a set of best practice principles. The principles clearly establish the audit committee's responsibility for maintaining the quality of the internal controls of the company. For many companies, a significant communication and understanding gap has developed between the Board/Audit committee and company internal audit/management. As a result, internal controls have subtly fallen off the agenda.

The CLERP 9 proposals also reinforce the need for a risk-based approach to managing a company's obligations. Before determining management strategies, a company should first establish what the risks are and then develop management strategies that will minimise the likelihood of the risks occurring. The Australian/New Zealand Risk Management Standard AS/NSZ 4360:1999 provides a very clear blueprint for making this happen.

This risk-based approach is entirely consistent with and reinforces the Privacy Commissioner's recommended approach. To establish an effective privacy response, first establish the risks via a risk assessment, then work to determine the best strategies for dealing with the risk. The Commissioner's advice to Transurban was to undertake a risk assessment[14].

The US equivalent to CLERP 9, Sarbanes-Oxley legislation goes much further. Every year, listed companies will be required to undertake an effectiveness audit of their internal control program. Compliance controls such as OHS and privacy will be a critical part of the review.

The challenge for the Privacy Commissioner: Sharing lessons

The private sector is poor at sharing lessons and best practices. We just have to look at the corporate governance debate for evidence. Despite being at the forefront of the corporate governance debate for many years during the early 90s, there is little publicly available best practice material on corporate governance in Australia directly relating to Australian

companies. Some 10 years on, the ASX has established the ASX Corporate Governance Council to develop best practice materials and standards for private sector governance.

My hope is that it will not take 10 years for best practice lessons on private sector privacy implementation to be developed and shared. Currently, apart from the sporadic survey of professional and industry members by active associations, there is little feedback or better practice information based on the Australian privacy experience readily available to the private sector. Although the OFPC does release updates or information sheets on topical issues these could not be described as sharing of private sector learnings or experiences with the implementation process.

It will be more than 18 months before the extension of the privacy legislation to the private sector is due to be reviewed and the outcomes reported. There is a clear need for the OFPC to be surveying participants, gathering better practice case studies and materials from private sector organisations to encourage increasing competence in management of personal information. The results would prove beneficial also to the next wave of private sector organisations to be covered by the Act with effect from 21 December 2002.

Conclusions

With the Privacy Act 1988 poised to cover small business from 21 December 2002, the implementation of privacy law across the private sector remains in its early stages. Over the past 18 months, through the effective approach taken by the Privacy Commissioner and his office, the private sector has been carefully prepared for the rollout of privacy laws. I believe we have witnessed one of the more successful and productive rollouts by a Commonwealth regulator.

To date, the private sector privacy rollout has been a good news story about building successful regulatory relationships. However, the final challenge is yet to be faced. How effective has the private sector been in implementing solid and enduring compliance programs into the many individual businesses and organisations? The indications from the ground is that there is still much to be done.

Endnotes

1 On 21 December 2001, the Privacy Amendment (Private Sector) Act 2000 (Cth) came into effect. It extended the Federal Privacy Act 1988 obligations to business with a turnover of more than $3 million and to health service providers, regardless of their size. On 21 December 2002, the Act was further extended to certain businesses under $3 million.
2 Chartered Secretaries Australia Ltd, CSA Rapid Response Survey No 3 – May 2001, http://www.csaust.com/news/index.cfm?part=5&subpart=5&subpart=3 accessed 31 October 2001
3 Interestingly, this was to be in direct contrast to a later survey conducted shortly after the enactment of the Privacy Act in February 2002, whereby 77 per cent believed they had sufficient time.
4 *Privacy Act waits in the wings*, Mark Fenton Jones, *Australian Financial Review*, 6 November 2001.
5 Ernst and Young, National Compliance Survey, 2002 http://www.ey.com accessed 28 October 2002.
6 Chartered Secretaries Australia Ltd, *CSA Rapid Response Survey No 3 – May 2001*, http://www.csaust.com/news/index.cfm?part=5&subpart=5&subpart=3 accessed 28 October 2002.
7 http://www.privacy.gov.au/media accessed 27 October 2002.
8 Methodoligies consistent with the Australian/New Zealand Risk Management Standard 4360:1999 are most common.
9 http://www.privacy.gov.au/media accessed 27 October 2002.
10 *Privacy Claws*, Sue Cant and Garry Barker, *The Age* 4 December 2001.
11 Sharpe, Brian *Making Legal Compliance Work*, (1998) CCH Australia
12 Australian/New Zealand Standards AS/NZS 3806: 1998, 7799.2:20000, 4400-1995, 4369:1999; OFPC Information Sheets, http://www.privacy.gov.au/publications.
13 Ernst and Young, National Compliance Survey, 2002 http://www.ey.com accessed 28 October 2002
14 http://www.privacy.gov.au/media accessed 27 October 2002.