CHARTERED SECRETARIES
AUSTRALIA

Leaders in governance

27 November 2007

The Executive Director
Australian Law Reform Commission
GPO Box 3708
SYDNEY NSW 2001

By email: info@alrc.gov.au

Review of Australian Privacy Law
Discussion Paper 72

Chartered Secretaries Australia (CSA) welcomes the opportunity to comment on the Australian Law Reform Commission (ALRC) discussion paper: *Review of Australian Privacy Law*.

CSA is the peak professional body delivering accredited education and the most practical and authoritative training and information on governance, as well as thought leadership in the field. Our members are all involved in governance, corporate administration and compliance with legislative and regulatory obligations, including those under privacy legislation at both Commonwealth and state levels, and as such are fully aware of their statutory obligations to maintain the security of personal information.

In representing the company secretaries of most of Australia's largest public and private companies, all of whom are responsible for maintaining registers of members and shareholder relations, CSA is also well placed to comment on the issue of shareholder privacy, which is raised in this submission.

An executive summary of the issues we raise for consideration is provided. This is followed by further detail on each issue that we raise.

Yours sincerely

Tim Sheehy
CHIEF EXECUTIVE

Executive summary

In this submission, CSA members focus on issues closely aligned to their areas of responsibility, rather than commenting on all issues raised in the discussion paper or issues of broader community concern. In brief, our submission canvasses issues relating to:

1. shareholder privacy
2. the transfer of personal information in corporate reconstructions
3. the notification of affected individuals of a breach of privacy, which we support in principle but which raises issues of practical implementation.

CSA supports the ALRC proposal that there be Unified Privacy Principles based on those that apply to private sector organisations and that state and territory governments should adopt the new Unified Privacy Principles.

CSA also supports the ALRC proposal that there should be a further review of privacy laws within five years of implementation of the ALRC's recommendations, and that if the proposed approach has failed to achieve national consistency, the Australian Parliament should consider overriding all state and territory privacy legislation to ensure consistency.

1 Shareholder privacy

There is a stark contrast between the protection of investors' privacy in bank accounts and superannuation and their lack of privacy in shareholdings. The Corporations Act is out-of-date in relation to privacy rights in operation for Australians, and not aligned with the obligations to protect privacy relating to other forms of financial information. Australians have a right to privacy in relation to their wealth holdings in bank accounts, yet retail and individual shareholders cannot prevent public disclosure of their wealth holdings in shares. There are also strict privacy requirements protecting investors in relation to superannuation contributions, which also contrast starkly with shareholders' lack of privacy.

CSA recommends providing increased privacy and protection to shareholders in relation to access to and use of their details on the register of members and removing the current provisions of the Corporations Act which permit any person to have access to the personal information of shareholders kept on a company's register of members. This would bring the Corporations Act into line with privacy obligations in place for all other financial dealings undertaken by Australians. While CSA understands that the principal law that the ALRC is reviewing is the Privacy Act 1988, CSA believes that the ALRC should support the extension of privacy rights to shareholders under the Corporations Act to ensure their rights align with Australians' privacy rights under other legislation.

To achieve acceptable privacy rights, CSA recommends that personal information concerning a shareholder should be subject to the same privacy principles as other personal information held by a company and in particular that companies should only:

- use shareholder information for the primary purpose for which it is provided — that is, administering a shareholder's shareholding — and for secondary purposes related to the primary purpose or to which the shareholder has consented
- disclose shareholder information to third parties with the shareholder's consent or as required by law.

2 Transfer of personal information in corporate reconstructions

CSA recommends that a company involved in a corporate reconstruction — typically a scrip takeover, demerger, asset split or other scheme of arrangement — be permitted to provide a shareholder's tax file number and payment instructions to the entity in which the shareholder receives shares as part of the corporate reconstruction.

3 Notification of affected individuals of a breach of privacy

CSA recommends that more specificity is required as to:

- the degree of certainty required as to the likelihood of a breach before the notification requirement is triggered
- exactly what constitutes 'a risk of serious harm'
- the permitted means of notifying affected individuals of a breach — in some cases an announcement to the ASX or a public advertisement may be the most practical or only way of notifying affected individuals.

Further detail on each of the issues outlined above follows.

1 Shareholder privacy

There is privacy legislation, at both Commonwealth and state level, designed to protect Australian citizens from the infringement of their privacy rights, yet the law relating to access to and use of the register of members (in the Corporations Act) does not meet acceptable privacy standards. CSA's concern at this lack of acceptable privacy rights is reinforced by regular complaints received by CSA members from shareholders angered that their personal details have been released to third parties without their consent or approval.

CSA believes the law requires reform to provide increased privacy and protection to shareholders in relation to accessing and using their details on the register of members.

Shareholders should have more acceptable privacy rights

While CSA understands that the primary law that the ALRC is reviewing is the Privacy Act 1988, CSA believes that the ALRC should support the extension of privacy rights to shareholders to ensure their rights align with Australians' privacy rights under other legislation.

CSA notes that, with the recent introduction of the Do Not Call Register, Australians can choose not to receive telemarketing calls in their home, even if their name and address is available in a public telephone directory. Yet shareholders in Australia cannot choose *not* to receive either predatory offers to purchase their shares or offers of an investment and advisory group's latest research report on the company in which the shareholder invests, which automatically places the shareholder on the investment and advisory group's client list, despite the shareholder not having agreed to such an inclusion.

Such offers come from offerors who argue that their request for information from the register is relevant to the shareholding and therefore within the Corporations Act s 177(1A) exemption. CSA members are concerned that such offers may well be predatory (below market value or on extended payment terms which effectively negate the value of the offer), yet under the current law, our members cannot refuse access to the register, even if they believe such offers to be for an improper purpose.

CSA recommends that personal information concerning a shareholder should be subject to the same privacy principles as other personal information held by a company and in particular that companies should only:

- use shareholder information for the primary purpose for which it is provided — that is, administering a shareholder's shareholding — and for secondary purposes related to the primary purpose or to which the shareholder has consented
- disclose shareholder information to third parties with the shareholder's consent or as required by law.

Existing law

The register of members has historically been a public register and indeed under s 173 of the Corporations Act 2001 the register is open to inspection by any member without charge and any other person on payment of such fee as may be prescribed. In addition, any person (whether or not a member) may require a copy of the register and, on payment of the prescribed fee, the company must provide the copy within seven days.

CSA contends that making all shareholders' details publicly available is an anachronism in the 21st century, when shareholders are no longer, as they were at the time of the introduction of the concept of limited liability, a small group of gentlemen in need of each other's particulars in order to confirm the application of a new concept. Today, shareholders can amount to millions

of geographically dispersed individuals participating in wealth acquisition. Modern technology makes the disclosure of shareholders' particulars vulnerable to predatory behaviour, in a way that is not possible with other forms of wealth holdings such as bank accounts and superannuation.

CSA supports existing specific grounds for access to the register

CSA fully supports the obligation on any shareholder with more than five per cent of shares (s 671B in Part 6C1) to publicly disclose their interest in the company. There are compelling public policy reasons why it is important for members and the general public to be able to understand the levels of control of any particular company. However, CSA cannot point to any public policy objective that is achieved by having all shareholders' details open for inspection on a public register and obtainable upon request.

CSA also fully supports the protection afforded to members to ensure they can:

- ask the company for a copy of the register (s 249E(3)) if they have convened a general meeting of members
- give a company notice of a resolution they propose to move at a general meeting (s 249N(1)). The company must ensure that all members receive notice of the resolution at the same time (s 249O(2)) and at the company's expense if the notice is received in time to send out with the notice of meeting (s 249N(3))
- distribute statements to all members on any matter that may be considered at a general meeting (s 249P(1)). The company must distribute it to all members (s 249P(6)) and at the company's expense if the statement is received in time to send out with the notice of meeting (s 249P(7)).

Such protections ensure that members can access or use the register for a proper purpose.

In relation to takeover bids, CSA notes that if a takeover offer has been made, it is subject to regulation as set out in Part 6 of the Act, which is designed to protect shareholders.

Retail and individual shareholders are primarily disadvantaged by the current lack of privacy

Retail and individual shareholders are the ones who are disadvantaged by the current lack of privacy. Shareholders whose shareholdings are held through a custodian company are largely protected from the general public accessing their particulars. Identifying these shareholders is feasible through the disclosure notice provisions in Part 6C.2 of the Corporations Act. However, this process of discovery is not the simple one of requesting a copy of a register of members, with full particulars.

As a result, those Australians with direct shareholdings, that is, predominantly retail and individual shareholders, are disadvantaged, despite the government encouraging Australians to invest directly. Thus the current situation makes it acceptable for some shareholders to have more privacy than others by virtue of how they structure their affairs. CSA contends that direct shareholders, with less complex structures in the management of their shareholdings, should have similar levels of privacy and protection to those whose shareholdings are held indirectly.

Recent legislation in the United Kingdom granting protection to shareholders

A proper purpose test has recently been introduced in the United Kingdom. The Companies Act UK provides that where a company receives a request for a copy of the register, it must either allow an inspection or provide a copy of the register or apply to the court. A company cannot simply decline a request. If the court is satisfied that the inspection, or copy, is not sought for a proper purpose, it directs the company not to comply with the request. It may also direct that the

company does not have to comply with similar requests. If the court considers the request to be for a proper purpose, the company must immediately allow the inspection or supply the copy.

CSA recommendations for reform

CSA recommends providing increased privacy and protection to shareholders in relation to access to and use of their details on the register of members. This would bring the Corporations Act into line with privacy obligations in place for all other financial dealings undertaken by Australians.

To achieve acceptable privacy rights, CSA recommends that third parties (including other shareholders) should only have access to or a right to obtain copies of personal information concerning a shareholder on the share register:

- if the disclosure relates to a substantial shareholder of the company (a five per cent or greater holding)
- to permit the company to make disclosures to the ASX in respect of directors' shareholdings
- where the person seeking access has lodged a bidder statement with ASIC in connection with a takeover of the company
- where the person seeking access is exercising a right to convene a general meeting of members or to distribute a statement to all members of the company
- where ASIC or the courts directs that a person is given access to or a copy of the register. ASIC or the courts could then be asked to apply a proper purpose test similar to the one in operation in the United Kingdom.

2 Transfer of personal information in corporate reconstructions

General comments

CSA notes that the current Privacy Act 1988 does not provide for the personal information in respect of shareholders that is already held to be transferred in corporate reconstructions, for example, in a scrip takeover, demerger, asset split or other scheme of arrangement, or when shares are received following a compulsory acquisition.

CSA strongly supports the principle that direct banking instructions and tax file numbers of individuals be closely guarded. However, CSA notes that in a corporate reconstruction a shareholder's existing investment is being transformed into a slightly different investment, yet the underlying privacy principles relating to that investment continue to apply. If a shareholder has not sold his or her shares at the time of a takeover, demerger or corporate break-up, the shareholder is clearly comfortable retaining the investment.

On this basis, the shareholder, having made a conscious decision to provide their payment details and tax file numbers in respect of the investment, expects that the personal information they have provided to allow them to benefit from their shareholding will continue to be utilised following the corporate reconstruction. CSA members note that many shareholders do not resupply information concerning their payment instructions and tax file numbers at the time of a corporate reconstruction, despite being requested to do so, as they believe the information, being already held, can be transferred without difficulty.

Impact on shareholders when transfer of personal information is not permitted under privacy legislation

CSA notes that there is *no* adverse impact on the individual in permitting the transfer of personal information in a corporate reconstruction.

However, CSA can point to a number of adverse effects on the individual when personal information is *not* permitted to be transferred in a corporate reconstruction.

CSA notes that seeking consent — consent that has already been provided by the shareholder — from shareholders concerning payment instructions and tax file numbers in corporate reconstructions imposes a cost not only on the company, but also on shareholders.

The cost imposed on shareholders is not simply that of the time that it takes for them to resubmit identical information for identical purposes to the same share registry. The unintended consequence is that the cost of seeking such identical information is ultimately born by shareholders as owners of the company. When the share registries of large listed entities are involved in corporate reconstructions (as in the current transfer of shareholders from Coles to Wesfarmers), the costs to shareholders inherent in the company contacting each shareholder to seek a resupply of information is significant. This cost is exacerbated by the fact that the company frequently needs to contact shareholders on more than one occasion, given that many shareholders do not supply the information as they believe it should be transferred automatically. Again, CSA stresses that this cost is borne by shareholders as owners of the company.

Not permitting a transfer of personal information in corporate reconstructions may also lead to additional costs to and inconvenience for shareholders, as the company will have to withhold tax on dividends if the tax file number is not provided. This may limit a shareholder's capacity to participate in a dividend reinvestment plan.

Given that many shareholders assume that their personal information can be transferred automatically and therefore do not resupply the personal information they have provided previously, such tax liabilities can affect large numbers of shareholders.

CSA recommendations for reform

CSA recommends that a company involved in a corporate reconstruction — typically a scrip takeover, demerger, asset split or other scheme of arrangement — be permitted to provide a shareholder's tax file number and payment instructions to the entity in which the shareholder receives shares as part of the corporate reconstruction.

CSA also recommends that shareholders should be able to request that the new entity destroys the information if for whatever reason the shareholder would prefer that the new entity should not hold this information.

3 Notification of affected individuals of a breach of privacy

The ALRC proposal

The ALRC discussion paper proposes that:

> The *Privacy Act* should be amended to include a new Part on data breach notification, to provide as follows:
>
> (a) An agency or organisation is required to notify the Privacy Commissioner and affected individuals when specified personal information has been, or is reasonably believed to have been, acquired by an unauthorised person and the agency, organisation or Privacy Commissioner believes that the unauthorised acquisition may give rise to a real risk of serious harm to any affected individual.
>
> (b) An agency or organisation is not required to notify any affected individual where:
>
> (i) the specified information was encrypted adequately;
>
> (ii) the specified information was acquired in good faith by an employee or agent of the agency or organisation where the agency or organisation was otherwise acting for a purpose permitted by the proposed Unified Privacy Principles (provided that the personal information is not used or subject to further unauthorised disclosure); or
>
> (iii) the Privacy Commissioner does not consider that notification would be in the public interest.
>
> (c) Failure to notify the Privacy Commissioner of a data breach as required by the Act may attract a civil penalty.

General comments

CSA members acknowledge that even the most security-conscious organisation or agency can become the victim of information theft and that many overseas jurisdictions have implemented legislative requirements for organisations and agencies to notify affected persons of data security breaches regarding their personal information. CSA also acknowledges that the proposed notification of breach of privacy can improve accountability, openness and transparency in the handling of personal information by agencies and organisations.

CSA generally supports the addition of provisions to the Privacy Act to require agencies and organisations to advise affected individuals of a breach to their personal information in certain circumstances and for Australian legislation to be aligned with global requirements on this issue. However, our support is conditional on:

- further guidance on how the provisions will respond to different levels of security breach (trigger notification)
- further guidance being provided concerning the test proposed by the ALRC to allow the agency or organisation to investigate the data breach and make an assessment of whether the unauthorised acquisition may give rise to a real potential for serious harm to an individual, rather than requiring notification of any unauthorised acquisition of personal information.

CSA fully supports the ALRC proposals for exception and the proposal that the Privacy Commissioner should issue guidance on the type and standard of encryption he or she will generally consider adequate, and the factors he or she will consider in assessing whether an agency or organisation will be able to avail itself of this exception in the case of a data breach.

CSA concerns with lack of specificity in the proposal

1 Triggering events and thresholds for notification

CSA supports allowing the agency or organisation to investigate the data breach and make an assessment of whether the unauthorised acquisition may give rise to a real potential for serious harm to an individual. However, CSA notes that the ALRC's proposal provides for oversight by the Privacy Commissioner and that the ALRC believes it is preferable that the decision about notification is made in consultation with the Privacy Commissioner. The ALRC proposal is that the Commissioner be able to require notification where he or she believes that the unauthorised acquisition gives rise to a real risk of serious harm to any affected individual, even if the agency or organisation disagrees.

CSA is concerned that, while this appears to set a higher threshold for notification of breach of privacy, the responsibility for assessing what will give rise to a real potential for serious harm to an individual does not sit with the organisation or agency, as all breaches must be reported to the Privacy Commissioner in order to arrive at a consultative decision. CSA believes that this imposes a compliance burden on agencies and organisations.

In practice it is often not possible to ascertain whether there has been an unauthorised disclosure of personal information as a result of a breach. Moreover, a technical failure that involves a momentary and minor 'blip' in the overall security of a system should not require the same notification response as a breach involving the disclosure of a large number of credit card numbers and expiry dates. And while disclosure of information already in the public domain such as names and addresses appearing in the White Pages is unlikely to lead to a risk of serious harm, without thresholds being determined as to what constitutes a reasonable belief that there is a risk of serious harm to an individual, companies will be compelled to notify all breaches.

CSA recommends that more specificity should be provided as to the degree of certainty required as to the likelihood of a breach before the notification requirement is triggered.

CSA recommends that guidelines should be issued specifying those classes of data breach that do not have to be notified to the Privacy Commissioner.

CSA also recommends that thresholds be determined for a reasonable belief as to what exactly constitutes 'a risk of serious harm'.

2 Timing and form of notification

CSA supports the ALRC proposal that it is preferable to allow for the method of notification to be determined by the agency's or organisation's ordinary method of communicating with the individual.

CSA supports the ALRC proposal that the Privacy Commissioner be empowered to approve substituted notice where he or she believes it is appropriate, reasonable and fair in all the circumstances.

CSA recommends that in some cases an announcement to the ASX or a public advertisement may be the most practical or only way of notifying affected individuals.

CSA recommendations for reform

CSA recommends that more specificity is required as to:

- the degree of certainty required as to the likelihood of a breach before the notification requirement is triggered (in practice it is often not possible to ascertain whether there has been an unauthorised disclosure of personal information as a result of a breach)
- exactly what constitutes ‘a risk of serious harm’ (for example, disclosure of information already in the public domain such as names and addresses appearing in the White Pages is unlikely to lead to a risk of serious harm)
- the permitted means of notifying affected individuals of a breach — in some cases an announcement to the ASX or a public advertisement may be the most practical or only way of notifying affected individuals.