Submission of Avant Mutual Group

on Australian Privacy Breach Notification

Date of Submission: 23 November 2012

Executive Summary

Avant Mutual Group Limited ("Avant") is Australia's leading medical defence organisation, offering a range of insurance products and expert legal advice and assistance to over 57,000 health practitioners and students in Australia. Our insurance products include medical indemnity insurance for individuals, practices and private hospitals, as well as life insurance and private health insurance through the Doctors' Health Fund, a member of the Avant Mutual Group. Avant develops and provides comprehensive risk advisory and education services to members. Avant has offices throughout Australia providing personalised support and rapid response to urgent medico-legal issues.

Avant welcomes the opportunity to provide this submission in response to the Commonwealth Attorney-General's Department's Discussion Paper "Australian Privacy Breach Notification".

For the reasons discussed in this submission, Avant's position is as follows:

1. A mandatory data breach notification law should not be introduced.

2. The current position of voluntary data breach notification in accordance with the OAIC's April 2012 Data Breach Notification guidelines should be maintained.

3. Moving to mandatory data breach notification would create a further and significant compliance burden with a corresponding increase in business costs, and business has had more than enough of this already.

4. We are not satisfied that there is any compelling evidence that mandatory data breach notification is necessary to achieve the stated goals.

Avant suggests that continuing and further education to ensure the proactive maintenance of privacy is preferable to a scheme that requires an organisation or individual to potentially incriminate themselves for a breach of privacy which could then be used as an admission in any investigation by the OAIC involving the breach.

In Avant's view the punitive approach of a mandatory obligation supported by civil penalties is unnecessary where an educative approach can achieve the same goals, and there is no evidence that such an approach has failed to have the desired effect.

Avant's Submission

Avant provides this submission in two capacities:

1. as an organisation that holds personal information including health information; and
2. on behalf of its members who hold health information.

The Discussion Paper seeks views on the following questions:

1. Should Australia introduce a mandatory data breach notification law?
2. Which breaches should be reported?
3. Who should decide on whether to notify?
4. What should be reported and in what time frame?
5. What should be the penalty for failing to notify when required to do so?
6. Who should be subject to a mandatory data breach notification law?
7. Should there be an exemption for law enforcement activities?

Should Australia introduce a mandatory data breach notification law?

Avant is strongly of the view that Australia should not introduce a mandatory data breach notification law, and that the current voluntary data breach notification arrangements and sanctions are sufficient to achieve the stated goals.

Avant agrees with the points set out in the discussion paper for retaining the existing position of voluntary data breach notification to the OIAC. We wish however, to highlight the following matters:

1. Reference is made to a number of significant privacy breaches in the introduction to the discussion paper. Only two of these examples appear to relate to companies operating in Australia.
2. In the examples of significant privacy breaches given in the introduction to the discussion paper, there is no suggestion that the companies did not act responsibly in response to the breach of privacy.
3. There is no evidence that Australian companies are not acting responsibly when it comes to notifying the OAIC and/or an affected individual of a data breach if there is a real risk of harm to the individual.
4. It would be onerous in these circumstances to introduce a nation wide data breach notification system as a result of the occasional few serious and wide ranging breaches, in relation to which there has been an appropriate response by the entities involved in the breach.
5. Avant's members often operate in solo practice and in small group practices. They are not multi-national and/or large companies. Accordingly, if a data breach notification system were introduced, Avant's members could suffer financially. Introduction of an audit and compliance system would be costly to small practices and this cost would no doubt be passed onto the public via increasing health costs.

6. Avant and its subsidiary the Doctor's Health Fund would have to institute a new audit and compliance program which could impact on the premiums charged to members and distract management from their primary task of looking after members.

7. The discussion paper reports that the OAIC was notified of 56 data breaches in 2010/2011, the equivalent of one per week and this is up from 44 in the previous year, an increase of 27 per cent. There are no details about the nature of these data breaches. These numbers are extremely small for an economy the size of Australia's. It would be reasonable to expect that if there were significant data breaches occurring with any greater frequency in Australia, then there would be far more voluntary reporting and/or complaints about such data breaches. The fact that the OAIC was notified of 56 data breaches during the 2010/2011 financial year, and opened 59 investigations into breaches where there was no notification is testament to the success of the current system. In these circumstances Avant submits that significant and wide ranging data breaches are not occurring, and that therefore there is no compelling evidence justifying introducing a nation wide mandatory privacy breach notification scheme.

Response to the Rationale for Mandatory Data Breach Notification Laws

Avant is strongly of the view that the stated rationale for mandatory data breach notification laws is being, and will continue to be, achieved through the current voluntary data breach notification regime and privacy breach sanctions, and that a mandatory scheme would be a disproportionate measure.

Mitigation of Consequences of Breach

There is no evidence that a mandatory data breach notification law is better than the current voluntary notification scheme in terms of mitigation of the consequences of a breach of privacy.

The introduction to the Discussion Paper refers to the ALRC's overall concern with identity theft, and notes that a notification requirement on entities that suffer data breaches would allow individuals to take remedial action to lessen the impact of the data breach.

As an organisation, Avant takes its privacy obligations seriously. Avant would have no hesitation in contacting an individual if there was a risk of harm, whether via identity theft, or in any other way. As noted above there is no evidence that organisations are avoiding such responsibility when there has been a data breach.

Avant's members, who have their patients' records and private health information entrusted to them, also take their responsibilities very seriously. As well as having a statutory duty of privacy, Avant's members have an obligation of confidentiality to their patients which is the cornerstone of the doctor-patient relationship. A breach of confidentiality or privacy can have a significant negative impact on the doctor-patient relationship. Similarly a failure by a doctor or medical practice to mitigate the consequences of a serious privacy breach and a failure to advise a patient of a serious breach may also have a significant negative impact. The potential of the doctor-patient relationship to break down and the associated reputational damage is sufficient reason for healthcare practitioners to take steps to mitigate the consequences of a serious breach. Imposing a mandatory obligation on practitioners to report privacy breaches is therefore unnecessary. Further, the proposed requirement to report the breach to the OAIC may exacerbate the original breach particularly in the context of sensitive health information.

It is Avant's view that those in the best position to mitigate the consequences of a privacy breach are the organisations that hold the information and the individual/s to whom the information relates. Voluntary notification to individuals where there is a real risk of harm

as a consequence of the breach is supported so that the individual concerned can take steps to mitigate the breach.

The benefits of notification to the OAIC could be achieved by continuing the current voluntary scheme. Based on the current voluntary notification guide, once notified, the OAIC's role is limited to providing guidance and advice on remedial steps that can be taken by an organisation. This is an educative function that in Avant's view can be achieved without a mandatory scheme.

Thus Avant submits that the mitigation goal can be achieved by providing more education to organisations about the voluntary data notification scheme and about remedial steps that can be taken once a breach has occurred.

Deterrence/Incentive to Improve Data Security

Avant takes very seriously its obligations to maintain the privacy of any information it receives in the course of its business.

In Avant's view the current and proposed processes and sanctions for privacy breaches are sufficient to act as a deterrent and as an incentive to improve data security. Current processes and sanctions include:

- complaint to the OAIC by an individual about a privacy breach
- the OAIC's ability to institute an investigation into a privacy breach on its own motion
- the OAIC's ability to inform the Minister of an action that needs to be taken to achieve compliance with privacy principles.

In addition, for Avant's members, breach of their statutory obligation to maintain privacy and of the duty of confidentiality may lead to disciplinary action, which may include a reprimand, fine and conditions being placed on the medical practitioner's practice of medicine. For example, a doctor may as a result of a breach of privacy have his or her practice audited by a regulatory authority such as AHPRA, the Medical Board of Australia or state-based privacy regulators. Such auditing is carried out at the expense of the medical practitioner and is a significant cost.

Further in Avant's view the new civil penalties for serious and repeated privacy breaches and the increased powers of the OAIC under the proposed amendments to the *Privacy Act* (contained in the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* are a sufficient deterrent and incentive to ensure the privacy of information. These increased powers include the ability of the Commissioner to conduct an assessment of an APP entity's maintenance of personal information, to accept written undertakings, and to include in a determination any order that is considered necessary.

Avant suggests that continuing and further education to ensure the proactive maintenance of privacy is preferable to a scheme that requires an organisation or individual to potentially incriminate themselves for a breach of privacy. This could then be used as an admission in any investigation by the OAIC involving the breach.

In Avant's view the punitive approach of a mandatory obligation supported by civil penalties is unnecessary where an educative approach can achieve the same goals, and there is no evidence that such an approach has failed to have the desired effect.

The ALRC recommendation relies heavily on the US position. However the ALRC notes that organisations in the US may not be subject to the same data security obligations as apply to Australian organisations under the *Privacy Act*.[1] Thus in the US the stated goal of

[1] *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108) paragraph 51.10

mandatory data breach notification as an incentive to improve data security holds more weight than in Australia where appropriate data security obligations exist.

Tracking of Incidents and Provision of Information in the Public Interest

The introduction of mandatory data breach notification simply to provide the OAIC with the ability to track incidents and yield information about privacy breaches, in circumstances where the vast majority of all privacy breaches would no doubt be minor and insignificant, is uncalled for and would place an unreasonable burden on the Australian business community, Avant and Avant's members for questionable gain, if any.

Maintaining Community Confidence in Legislative Privacy Protections

The discussion paper states that having a system where all breaches of privacy are reported, even if the breach is minimal, may bolster public confidence that government is taking individual rights seriously. Avant submits that there is no evidence that members of the public currently feel disempowered and/or would feel empowered if, for example, a minor data breach notification was reported to the OAIC. The introduction of a mandatory data breach notification system on the basis that it may bolster public confidence is speculative at best.

Mandatory data breach notification may also cause an individual harm and/or unnecessary distress and would be unwarranted if the breach was minor and had been corrected with no harm caused to the individual.

General comments

The Discussion Paper assumes that the organisations to which mandatory data breach notification would apply are Commonwealth agencies and large private sector organisations[2]. Large companies can be expected to have sophisticated privacy compliance programmes and policies that apply if there were a data breach. However the *Privacy Act* also applies to health care providers that hold health information, even if those providers would otherwise be a small business or small business operator. The compliance burden associated with mandatory data breach notification for these organisations would be significant, and would include costs associated with privacy audits, staff training and the like. Considerable resources would be needed by organisations to set up and maintain systems to monitor unauthorised privacy breaches at this very specific level. There is, however, no reason and no fair way to differentiate between larger and smaller companies and in any event it would in most cases be the Australian public that would bear the cost of the new compliance systems that would be needed.

There is also the issue as to how the OAIC will deal with the volume of notifications if all data breach notifications, no matter how minor or insignificant, are to be reported to the OAIC. An example is if an employee of an organisation were to access the personal records of a customer on an unauthorised basis but with no personal information being disclosed to anyone outside the organisation in question. This breach is clearly best left to the entity to deal with either by way of further education and/or possibly disciplinary action against the employee.

There is the potential for the OAIC to be overwhelmed by the notification of many privacy breaches as there would be a potential bias towards over-notification for fear of the sanctions for not doing so.

Avant submits that the OAIC's resources could be better spent on an education program rather than a mandatory data notification scheme.

[2] Discussion Paper Australian Privacy Breach Notification page 16.

Avant contact details

Should you have any further queries in relation to this submission, please contact:

Georgie Haysom
Head of Advocacy
Avant
Telephone: 02 9260 9185
Email: Georgie.haysom@avant.org.au