4 March 2016

Commercial and Administrative Law Branch
Attorney-General's Department
3-5 National Circuit
BARTON ACT 2600

privacy.consultation@ag.gov.au

Consultation: draft serious data breach notification bill

Thank you for the opportunity to provide this submission regarding the **draft serious data breach notification bill** (the **Bill**).

Introduction

The Association for Data-driven Marketing & Advertising (ADMA) represents the full 360 degrees of Australia's media, marketing and advertising ecosystem. ADMA itself is the principal industry body for data-driven marketing and advertising in Australia. Data-driven marketing and advertising is platform neutral and includes any marketing communication which uses data-insights, including personal information, to engage with a consumer with a view to producing a tangible and measurable response.

In addition, ADMA powers the Institute of Analytics Professionals of Australia (IAPA) and the Australian Interactive media Industry Association of Australia (AIMIA). For the purposes of this submission the associations are collectively referred to as the ADMA Associations.

ADMA's primary objective is to help companies achieve better results and efficiencies through the enlightened use of data-driven insights. ADMA serves its members interests by protecting, supporting and championing excellence in data-driven marketing and advertising in Australia and beyond. Originally the Australian Direct Marketing Association, ADMA evolved with the times and became the Association for Data-driven marketing and advertising. Where our previous focus pertained to initiatives such as the *Spam Act* and the Do Not Call Register we now have a much broader remit which encompasses digital, data, security, communications, media and convergence within those areas.

In excess of 750 member organisations from a broad spectrum of Australian industries belong to the ADMA Associations and we have a subscriber base of over approximately 38,000 individuals. Members range in size from SMEs to multinational corporations. They include banks and telecommunications companies, advertising agencies, specialist suppliers of marketing services, statutory corporations, retailers, specialist industries such as travel and automotive, charities (both large and small) and educational institutions.

Almost every Australian company and not-for-profit organisation markets to its current and potential customers using data-driven insights as a normal and legitimate part of its business activities. The ability to continue to conduct this activity underpins a large proportion of Australia's economic activity.

The importance of the digital economy for the future of Australia cannot be understated and this notion has been embraced by the marketing and advertising community and incorporated into its lexicon. In March 2015, Australia's digital economy was valued at $79 billion or 5.1% of its gross domestic product[1].

Digitisation represents both the now and the future for ADMA and its members and we have a vested interest in ensuring that the right regulatory framework is in place to enable Australia to progress into the future.

General comments regarding the Bill

In simple terms ADMA's position is that:

(a) There has been no evidence provided to establish that there is an imperative for the proposed provisions. The Office of the Australian Information Commission (OAIC) has had voluntary breach notification guidelines in place for some time and, as far as we are aware, there is no evidentiary basis that establishes the need for the legislation.

(b) The Bill is the latest is a series of attempts to pass mandatory breach notification provisions for serious data breaches. Leaving aside the issue of whether the proposed legislation is needed in the first place, the current iteration of the regulatory provisions does little to address previous concerns.

(c) There is the potential for the scope of the legislation to be increased via regulation and, in doing so, to dispense with the "serious data breach test".

(d) The Bill has the potential to cause "notification fatigue".

[1] Deloitte Access Economics, *The Connected Continent II - 2015*

Detailed submissions

Expanding on each of the points above in turn:

A. No imperative for the legislation

Legislation is designed to cure ills and to protect. Both this, and the previous government, has failed to explain why this legislation is needed and why the voluntary reporting regime is not sufficient.

The *Privacy Act 1988 (Cth)* already mandates the protection of personal information (Australian Privacy Principle 11). However, the Act does not mandate the notification of breaches. The Bill purports to ensure that individual can take remedial steps to avoid or minimise potential loss or harm in the event that the person information is compromised.

The reality is that the OAIC voluntary guidelines already in place are being adopted by industry effectively as consumer sentiment is a key driver of business success and businesses seek to ensure that their relationship with consumers is one that is built on trust.

Business has repeatedly questioned the justification for the proposed legislation. To proceed with the legislation adds to the already significant compliance burden faced by business and this is diametrically opposed to the government's own stated objectives of increased productivity and reduced red-tape.

We question how the Bill is consistent with the Government's own Regulatory Performance Framework[2], particular KPI's 3 and 6 of those listed below.

> KPI 1 – Regulators do not unnecessarily impede the efficient operation of regulated entities
> KPI 2 – Communication with regulated entities is clear, targeted and effective
> KPI 3 – Actions undertaken by regulators are proportionate to the regulatory risk being managed
> KPI 4 – Compliance and monitoring approaches are streamlined and coordinated
> KPI 5 – Regulators are open and transparent in their dealings with regulated entities
> KPI 6 – Regulators actively contribute to the continuous improvement of regulatory frameworks

With respect to KPI 3, ADMA does not for a moment contend that data breaches are not a serious issue however we assert that the risk is already being well managed. In ADMA's view the introduction of the Bill is not only unnecessary but may have negative implications for consumers (as discussed below).

[2] https://www.cuttingredtape.gov.au/resources/rpf

B. Previous drafting issues have not been resolved

This Bill, and its predecessors, have a long and chequered history – it has been considered by parliament before (as a different iteration) but was criticised for vagueness and lack of meaningful detail. The last Bill ultimately lapsed and nothing came of it.

ADMA is concerned that the Bill is still too vague. Vagueness leads to conjecture and prevents business from addressing regulatory requirements with certainty and efficiency. This in turn decreases productivity and increases cost.

C. Definition of "real risk of serious harm"

The types of "serious harms" identified have been expanded and notification provisions have ben clarified to so that if an entity suspects but is not sure that such a breach has occurred then they have 30 days to determine whether notification is required.

However there are still challenges with definitions. The Bill defines a "serious data breach" as one that creates a "real risk of serious harm" to affected individuals. In turn, a "real risk" is defined as being "not a remote risk". Given that "remote risk" is not defined this type of circular definition is not helpful.

Although the definitions are drawn from the current voluntary regime enshrining such vague definitions in legislation will only serve to drive business to adopt an overly cautious approach to reporting which in turn is likely to result in notification fatigue (discussed at "E." below). In addition, the increased regulatory burden will result in a corresponding increase in the cost of doing business – a cost that will ultimately be borne by the consumer.

D. Potential to broaden the scope of the legislation exponentially via regulation

The inclusion of a provision allowing regulation to mandate notification of breaches without the application of the threshold test of there being a "serious data breach" appears to have gone completely unnoticed. The accompanying Explanatory Memorandum[3] contemplates the application of this provision and posits a scenario relating to health records. ADMA agrees that health records should be afforded the highest level of privacy protection but questions why the application of the serious harm test should not apply?

E. Notification fatigue

As it stands the proposed legislation will impose an unnecessary compliance burden on industry, this in turn will increase the cost of doing business which almost inevitably will impact on consumers. The vagueness of the provisions is also likely to result in businesses erring on the side of caution and issuing notifications for any actual or potential breach – this would result in notification fatigue with the messages becoming "white noise" to consumers. Ironically this has

[3] Explanatory Memorandum at 7, page 3

the potential to leave consumers more exposed than they are presently as they may pay less attention to the notifications.

Closing comments

Regulation needs a cautious hand, as otherwise we may find that over-regulation serves only to detract from its intended purpose by causing confusion and creating an unnecessary burden.

ADMA thanks the Attorney General's Department for the opportunity to provide input regarding the Bill.

As the ADMA Associations constitute the preeminent Australian association for data-driven marketing and advertising, digital marketing and data analytics, we would welcome the opportunity to discuss the proposed Bill further with the Department or to play a role in any further consultation.

Yours sincerely

Jodie Sangster
Chief Executive Officer
ADMA
e: jodies.sangster@adma.com.au

Jeannette Scott
Director - Legal & Regulatory Affairs
ADMA
e: jeannette.scott@adma.com.au