ADMA Association for data-driven marketing & advertising

20 June 2013 Submission to:

Senate Legal and Constitutional Affairs Legislation Committee consideration of:
PRIVACY AMENDMENT (PRIVACY ALERTS) BILL

ADMA Concerns about Inadequate Consideration of Implications

The Association for Data-driven Marketing and Advertising, representing more than 550 corporate members, wishes to bring to the attention of Senators its serious concerns about the proposed positive reporting regime contemplated in the above bill that has been referred for consideration by this Committee. In the very short amount of time that has been provided for consultation with our members, we have identified a number of issues with the Privacy Alerts Bill.

Our concerns are summarised as follows:

1) Failure to follow the Government's promised process for privacy reform.
2) The Bill is being unnecessarily rushed through Parliament without proper consultation with private sector stakeholder who face significant additional costs and compliance red tape.
3) Imprecise and vague wording of key terms such as 'serious harm' on which important risk mitigation decisions depend.
4) Failure to demonstrate a clear public benefit to justify the additional compliance burden on small and large business.
5) Compliance costs to be passed through to consumers and result in higher prices for goods and services, and loss of competitiveness and innovation for Australian businesses.
6) Poor resource planning to deal with the spike in reporting bureaucracy.
7) Ill-advised additional powers to appointed, unelected officials, including the power to impose legislative mechanisms without reference to Parliament.
8) No evidence of systemic failure to justify a positive reporting regime.
9) Unfair exemption for political parties.
10) Failure to deal with fraud matters.

Failure to Adhere to Agreed Process of Consultation

The Federal Government previously committed – and industry and other stakeholders agreed – to a rational, three-stage process of consultation on privacy law reform. The stages involved:

1. New administrative arrangements with the establishment of the OAIC
2. Consultation and consideration of the first tranche of ALRC privacy recommendations
3. Consultation and consideration of the second tranche of ALRC recommendations including Mandatory Data Breach Notification (MDBN)

However, proper process has been replaced by haste, ill-considered legislation, and regulatory overload. The hurried passage through the lower House of the Privacy Amendment (Privacy Alerts) Bill is a prime example of the breakdown in the information privacy decision-making process.

Request that the Bill be Referred for Proper Consultation with Industry
ADMA is requesting that the Bill be shelved until concerns of business have been given proper consideration. I attach a submission that summarises our concerns. We appeal for your support and assistance in ensuring that this ill considered and flawed legislation does not pass into law.

RECOMMENDATION: ADMA wishes to put on the record its strong objections over the extremely short period of industry consultation which has made it impossible to properly gauge the significant macro-economic impacts of this new reporting regime. It recommends that the Committee refer the legislation for proper consideration to an appropriate Committee of Parliament.

Lack of Definition of 'Serious Harm' will Result in Reporting of Frivolous Matters
In its current form, the legislation fails to define a key term 'Serious Harm' which will trigger the reporting of breaches. This is a significant flaw that must be addressed before the Bill becomes law. In the short time available to consider the legislation, it has been impossible to quantify the likely costs involved is assessing 'serious harm' however they are certain to be passed along to consumers in the form of higher costs for products and services.

RECOMMENDATION:
It is our view that the legislation should be subject to thorough review by the Committee including public hearings.

The ALRC recommendations that gave rise to this bill were not put through a proper process of consultation with industry, therefore the definition of 'serious breach' or 'serious harm' has not been worked through. Nor have many other industry concerns about MDBN been considered. We recommend that this matter be referred to the ALRC as part of its new privacy reference and that a proper consultation process be undertaken before the legislation is given further consideration by Parliament. This would be a relatively small addition to the terms for the pending ALRC reference.

Risk of Over-reporting of Defeats Aim of the Bill
The absence of a clear definition of 'serious harm' in the legislation will likely cause organisation to become extra cautious about potentially breaching the obligation and so default to the most risk-averse internal policy setting. This, in turn, will lead to the over-reporting of relatively minor data-related errors, as compliance managers act to protect their organisation's reputation.

According to recent research by McAfee (cited by Minister Dreyfus in a speech to a Privacy Reform and Compliance Forum in Sydney 12 June) around 21% of Australian businesses have suffered data breaches. In 2012 there were 2,141,280 businesses trading in Australia. That means the Privacy Commissioner can expect to be investigating 449,669 potential data privacy breaches once mandatory positive reporting takes effect.

Dumbing-Down of IT Security Systems
In a recent report in Fairfax media, an IT expert has warned that the legislation could actually have the perverse effect of "dumbing-down" the security around personal data, especially for smaller businesses that do not have sophisticated data management systems:

> "…consulting firm Securus Global chief executive Drazen Drazic believes the legislation will have little effect where it is most needed – on poorly protected firms who do not properly monitor their systems for attacks. Advertisement

Drazic told IT Pro the government had approached the issue the wrong way around. It should have legislated minimum standards of security in order to establish a level playing field.
"The idea of a base level equal playing field throws a spanner into the works and turns something relatively simple into a larger, broader and more complex strategy - but overall a better one," he said.
The new rules create an uneven playing field, he wrote in a blog post.
In their current form the rules hurt organisations who detect more breaches, Drazic argued, which are most likely the firms with good security practices and accurate monitoring capabilities.
The new laws would force these security-conscious businesses to disclose more breaches while "clueless" companies, who don't know they been attacked, could simply plead ignorance.
"A better, more secure company, who knows what is happening in their IT environment, is in more danger of being negatively impacted than a less conscientious company," he said.
This meant the new legislation would not improve the quality of security through transparency. It could see companies "dumb down" their logging and monitoring capabilities, as well as governance, so they did not detect breaches in the first place. Therefore there would be fewer breaches to report, protecting their reputation.
"Without a level playing field, their less secure competition can plead ignorance to understanding whether a breach has occurred," Drazic said.
"So why continue the expense involved ... it would make better business sense to dumb down and minimise the risk of being put into a position of public breach disclosure."

http://www.smh.com.au/it-pro/security-it/privacy-breach-laws-may-prompt-companies-to-dumb-down-monitoring-20130619-2ohyg.html

Proactive versus Reactive Compliance Systems

Regulatory compliance systems across all business are normally set to react to evidence of breach, usually triggered through complaints or internal audit. The proposed MDBN regime will require organisations to move from a 'reactive' to a 'proactive' default compliance setting. In practice, this means organisations will need to divert enormous IT and legal compliance resources to the task of searching out and reporting data management errors that may or may not indicate 'serious breach'. Again, since 'serious breach' is not defined, the default settings for these new systems will have to be very high in order to mitigate the risk of serious financial penalty and reputational (brand) damage, which would inevitably follow from an investigation by the OFPC.

Costs and added Compliance Burden

More than half of ADMA's members are small to medium sized enterprises or not-for-profit organisations. The costs of MDBN will fall relatively more heavily on small entities which do not have internal resources dedicated to regulatory affairs. Because many are data-driven organisations, they will not be able to avail themselves of the small business exemptions in privacy law.

In relation to SMEs, MDBN will impose a disproportionate cost on small businesses and start-ups, the innovators of the Australian digital economy. It will increase perceived business risk which will have a flow-on effect on decision-making (risk aversion) and increase insurance and compliance costs.

While the obvious answer is for businesses to implement strong processes to prevent any data breaches, it's not always that simple. Unfortunately this process could result in businesses spend more time managing the reporting process itself and less time actually managing the right outcome for customers.

Significant New IT Costs

Meanwhile, the additional requirements of mandatory notification will involve significant IT capital expenditure for larger and/or data-dependent organisations. These costs will vary depending on the amount of data held by the entity but will easily run into the millions of dollars. Similarly the cost of notification will depend on the size and nature of the breach.

Commencement in less than a year – as would be the case with commencement in line with the Enhancing Privacy Protection amendments – will obviously involve the extra costs of unbudgeted and unexpected expenditure on capital and human resources.

Lack of Public Benefit to Offset Costs to Business
The Regulatory Impact Statement (RIS) associated with the Bill is woefully inadequate in assessing the true cost to the Australian economy of these measures. The benefit to the public is not in proportion to the cost to business. The RIS offers no evidence that current voluntary disclosure arrangements, backed up by an enquiring news and social media, are providing insufficient protection to consumers. In relation to Not-For-Profits, charities and non-government organisations are going to have to brief consultants and engage law firms at considerable expense, which will draw scarce financial and staff resources away from their core charitable activities.

No evidence of systemic failure
Although there have been data breaches from Australian companies and from international companies holding data about Australians, there is no evidence of widespread systemic failure or wilful misconduct. There is also no evidence that actual breaches have been dealt with unsatisfactorily under existing regulatory arrangements. After 12 March 2014 new protections will be in place. There is no justification for the introduction of additional mandatory measures at this stage.

Voluntary Disclosure Works
There are also many self-correcting mechanisms in the market. These include companies making announcements of their own volition, media disclosures and affected individuals taking actions themselves via social media or complaining to the OAIC. Companies with brand reputations to protect will fail to disclose data breaches at their peril.

Too Much Power to Regulators to Interpret Key Elements of Law
The failure to define key elements such as 'serious harm' will also give a free hand to the Regulator to interpret the legislation via regulation and use its new powers to impose punitive sanctions and Codes which will be a form of 'back-door' legislation without proper scrutiny by Parliament.

New Powers of the Commissioner to Impose Codes and Sanctions
ADMA contends that the data security measures contained in a combination of the new APP11.1, the enhanced powers of the OAIC and the existing voluntary Data Breach Notification Guide provide more than adequate protection for the types of breaches which have occurred to date.

ADMA is concerned that the ability of the OAIC to initiate the development of codes which will be legislative instruments may be tantamount to legislating via the back-door. If legislation is evidenced to be warranted, the matter should be subject to the usual legislative processes. The ability to circumvent the legislative process through regulator-imposed 'code development' – and then give the same weight to a code as the law – is deeply concerning.

Privacy Commissioner Not Resourced to Handle Additional Workload
Given that organisations are likely to take a risk-minimisation approach to compliance (ie err on the side of over-reporting data errors and potential breaches) and given the uncertainty of the application of the law and vague wording of terms like 'serious harm', the Privacy Commission is likely to be inundated with reporting and unable to cope with the internal red tape burden this initiative will trigger. At a recent Senate Legal and Constitutional Affairs hearing, the Australian

Information Commissioner indicated that the complaints backlog in the Privacy Commissioners Office is already significant and staffing was under resourced.

> Wednesday, 29 May 2013 Senate Page 77
> **Prof. McMillan:** In the budget papers there are projected completion rates. The objective is to complete 80 per cent of Information Commissioner reviews within 12 months of receipt and, equally, to complete 80 per cent of privacy and FOI complaints within 12 months of receipt. We are not currently meeting that objective, but that is what we will be focused on in the forthcoming year.
> **Senator RHIANNON:** How many additional staff would you need to achieve that objective?
> **Prof. McMillan:** We have not calculated an exact figure. We have obviously had discussions around budget. The Privacy Commissioner wrote to the Attorney-General drawing attention to the workload pressures imposed by the privacy reforms, but we have been well aware of government announcements and government measures, including the efficiency dividend, so we have not done scenario modelling. When the proposals for FOI reform and the creation of the office were going through the parliament it was projected that the office would have 100 staff under the departmental appropriation. That is a figure we have been comfortable to accept as a projected number. The numbers go up and down, but they will probably stabilise. They are currently down, under departmental appropriation, to around 64; it will probably stabilise in the next financial year at around 70

Failure of the Bill to Deal with Serious Fraud and Hacking Issues
Globally data breaches which cause serious harm are far more likely to be attributable to hackers and rogue operators than legitimate organisations. Mandatory notification in isolation places a disproportionate burden on organisations (which are also the victims of criminal activity) while doing nothing to address the fraudulent activity that actually causes the damage.

Wrong timing to be introducing MDBN
The timing is wrong for the following reasons:
1. Organisations are heavily involved in preparation for the start of the APPs, credit reporting and other Enhancing Privacy Protection amendments.
2. It is not possible for even large corporations and well-resourced Not-For-Profits to properly consider and adequately respond to the current requests for information and submissions from the Attorney-General's Department and the OAIC.
3. Questions have been raised in Parliament – and during Senate Estimates - about the OAIC's resources to cope with the extra work load arising from the Enhancing Privacy Protection amendments. It is clearly not timely to introduce additional requirements of the OAIC in respect of positive reporting.

Time Needed to Adjust
To provide a measure of certainty and consistency, the period between passage of the legislation and commencement should be a minimum of 15 months as has been the case with the Privacy Amendment (Enhancing Privacy Protection) Act 2012. This should not be read in any way as an endorsement by ADMA of the legislation. ADMA's position is consistent with that expressed in its submission to the MDBN discussion paper which was to oppose additional legislation and maintain the existing voluntary disclosure regime.

Political Parties Should Not be Exempt
There is no rationale for extending the exemptions enjoyed by political parties under the Privacy

Act to include matters of positive breach notification. If 'serious harm' flows from unauthorised disclosure of personal information held by a political party, it should be subject to the same sanctions and penalties that apply to other organisations.

About ADMA

ADMA is the principal industry body for data-driven, customer-centric, measurable marketing and advertising in Australia. ADMA's primary objective is to help companies achieve better marketing results through the enlightened use of data-driven insights into consumers.

Consistent with this objective, ADMA has been involved in the development of legislation, as well as co-regulatory and self-regulatory schemes, over many years. ADMA was formed in 1966 and has, during its 47 years of operation, been involved in the development of the Privacy Act 1988, the Spam Act 2003, the Competition and Consumer Act 2010, the Do Not Call Register Act 2006, the Privacy Amendment (Enhancing Privacy Protection) Act 2012, the ADMA Direct Marketing Code of Practice 2006 (based on the model code of practice endorsed by the Ministerial Council of Consumer Affairs in 2003), and the Australian eMarketing Code of Conduct 2005.

ADMA works closely with the other relevant industry associations to ensure that codes are consistent and provide comprehensive coverage across all channels. Cross-industry forums and alliances such as the Australian Marketing and Media Industry Forum, and the Australian Digital Advertising Alliance, provide a means for a consistent approach to tackling the challenges that exist in every regulatory environment.

ADMA has over 550 member organisations, including some of Australia's most well-known and trusted brands. Our members come from many industries including major financial institutions, telecommunications companies, energy providers, information and technology companies, digital service providers, travel service companies, major charities, statutory corporations, educational institutions and specialist suppliers of marketing services.

Data-driven marketing and advertising 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. Data-driven marketing is platform neutral. It includes marketing via:

- email
- mobile phones and other mobile devices
- apps
- online
- social media networks
- mail
- telephone calls
- print
- television and radio broadcast

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

Jodie Sangster, CEO
Association for Data-driven Marketing & Advertising

- End -