Mr Tim Bryant
Inquiry Secretary
Senate Legal and Constitutional Affairs Committee
PO Box 6100, Parliament House Canberra ACT 2600

Dear Mr Bryant

Thank you for the invitation of 19 June 2013 to make a submission regarding the *Privacy Amendment (Privacy Alerts) Bill 2013* (Cth).

In summary, there is international acceptance of mandatory data breach notification. Experience overseas demonstrates that

- there is a need for mandatory notification of breaches – what the Bill unfortunately characterises as 'Privacy Alerts'
- mandatory notification has been welcomed by a range of stakeholders, including consumers, business and regulators
- such notification has not imposed an excessive burden on public and private sector organisations that have experienced data breaches.

The Bill is deficient in several aspects and should accordingly be regarded as a first step towards best practice and consistency with emerging overseas standards. It is however a valuable first step and, subject to concerns identified below, I commend it to the Committee.

Basis

I teach privacy, confidentiality, secrecy and data protection (at the graduate and undergraduate levels) at the University of Canberra. I am General Editor of *Privacy Law Bulletin*, the leading privacy and data protection law practitioner journal, and over the past decade have published articles and presented papers directly relevant to the Bill. I am a member of the Australian Privacy Foundation, the salient civil society body concerned with privacy, and am a member of the OECD body concerned with the development of an effective framework for global health sector data protection.

The following comments are independent of the University of Canberra.

Notification

The Bill addresses a substantive and serious problem in a way that is of benefit to public policymakers, consumers, business and Australian courts.

The past decade has been punctuated by disclosure that some of Australia's leading organisations – alongside their public and private sector counterparts in the United States, the United Kingdom and other jurisdictions – have experienced the unauthorised exposure of personal information that in aggregate now relsates to hundreds of millions of people.

That exposure, generally labeled a data breach, has involved the University of

Sydney, Telstra (on a recurrent basis), Vodaphone, Sony, the US Veteran's Administration, insurers, banks, pathology service providers, medical clinics and hospitals, welfare bodies, hoteliers, major publishers, retailers, adult content payment services, airlines, accounting firms, security consultants and local government agencies.

The information has included detailed medical records, drug and other test results, personnel files, contact databases, payroll details, credit card lists and entitlement records. It is information that those organisations should and – importantly – **could** keep securely.

Data breach, particularly recurrent breach, is **NOT** inevitable and should be managed.

In some instances the exposure I have noted above is directly attributable to egregious poor information management within the organisations (exacerbated by failure to adopt security mechanisms such as encryption of databases) and to indifference on the part of executives when a breach is suspected or confirmed.

That indifference is understandable, given the

- absence of legal sanctions,
- unduly permissive stance of the Office of the Australian Privacy Commissioner (which has been notably reluctant to publicly 'name and shame', arguably because it has undergone regulatory capture rather than simply because it is under-resourced) and
- absence of a mandatory reporting regime.

On the basis of sporadic disclosure within Australia and mandatory reporting of breaches in the United States we can credibly infer that data breach **is** occurring in Australia and **is** often preventable. Unauthorised exposure of personal and corporate information is not a matter that is completely outside the control of public and private sector entities. Those entities should be encouraged to adopt a positive approach. The individuals or organisations that either have a choice or that are required to deal with those entities should have enough information to enable them to influence the entities.

The absence of mandatory reporting under Australian law means that we have no authoritative information about the

- frequency,
- scale and
- seriousness

of the Australian breaches. We should be concerned about breaches because they facilitate the identity offences that have received bipartisan attention over the past five years and because they erode consumer trust in public and private sector organisations that have been entrusted with personal and corporate data.

Mandatory reporting in Australia will provide solid information for the Australian Parliament, the Government, law enforcement bodies and industry regarding breaches. Policymaking should not be dependent on media coverage in the *Daily*

Telegraph, the *Australian Financial Review* and *IT News* or on anecdotal accounts by information technology staff.

There is a compelling public benefit in being able to identify what breaches are occurring and thereby, for example, enable consumers to encourage data custodians to embrace best practice.

At the moment some breaches are not being identified by organisations, ie they do not recognise that they have breached. Other breaches are identified by organisations but are not publicly revealed because disclosure would foster inconvenient questions about management practices. Disclosure might also encourage consumers to call for law reform and for the remedies that are apparent at both the state and federal levels in the United states and at the national level in the United Kingdom.

Feasibility

As indicated above, experience overseas demonstrates that mandatory data breach reporting has not fundamentally reduced the commercial viability of private sector organisations, has not imposed an onerous burden on government agencies and has been welcomed by a range of stakeholders.

I accordingly suggest that the Committee look critically at problematical claims that a data breach regime will necessarily be a major burden on business, will discourage organisations from best practice in information management or is neither desired nor needed by consumers. Mandatory reporting is one element of the legal system and information practice that is essential for the world of 'big data', 'the cloud' and emerging global privacy standards such as development in Europe under the auspices of the Article 29 Working Party or by the OECD in relation to health data.

A voluntary reporting scheme, such as that currently in place in Australia, means that many organisations will not alert anyone – particularly on a timely basis – about an actual or suspected breach, that vulnerabilities may be exploited by offenders over months or even years (as in some recent incidents) and that professional peers will not become aware of and thereby gain the authority to minimize breaches of the data collections and networks for which they are responsible. In essence, mandatory reporting is useful because it provides information to organisations that have not been breached, so that they do not assume 'breaches won't ever happen to us'.

The timeframe for a response to the Committee's invitation prevents a detailed response but my assessment, on the basis of tracking breaches and examining the operation of overseas mandatory breach statutes over several years, is that the 'Alerts' Bill does not represent best practice and that although it should become it will need to be amended by the end of the decade to reflect international developments and Australian business/consumer expectations. In that respect I draw your attention to briefings by the Australian Privacy Foundation.

The following paragraphs identify some specific concerns.

Specific Concerns

<u>Offshoring</u>

It is axiomatic that Australian law does not supersede the law in other jurisdictions. It is also axiomatic, however, that we should take responsibility for matters that are in our control and should discourage a sense that the intent of Australian privacy law (and specifically mandatory reporting) can be disregarded by going offshore. The reporting regime should cover breaches that are offshore but under Australian control.

That is consistent with the approach taken regarding spam and the Do Not Call regime. (I note that there were claims in parts of the information technology community that law regarding unsolicited commercial calls, faxes and email was unnecessary and undesired by consumers or would impose an onerous burden on business. Australia's experience has demonstrated the lack of substance in those claims.)

Exceptions

The effectiveness of the Australian privacy regime has been weakened since 1988 through exclusions and exceptions. It is important to be foreard looking and resist the temptation to enshrine and exceptions and excuses for non-disclosure after a data breach has occurred. The legislation should not be inappropriately restrictive; it should instead cover those entities that are covered by the Commonwealth's powers and should not take a narrow view of 'personal information' on the basis of medium or data type or construe harm solely in financial costs (ie should encompass mental harm or severe distress).

Supervision by the Privacy Commissioner of mandatory breach reporting should not be fundamentally weakened through scope for discretionary exceptions. For the purposes of public administration we should reduce the subjectivity that results in 'closed door' dealmaking – and requests for deals. Consistency and transparency will reinforce the credibility of the Office of the Information Commissioner, which has been eroded by perceptions that the organisation is either very permissive or naïve, for example in dealing with breaches in the telecommunications sector.

Compliance

The Government has regrettably disregarded recommendations by three law reform commissions, by parliamentary committees and by analysts in belatedly passing the hot potato known as the privacy tort back to the Australian Law Reform Commission. We should be acknowledging that breaches impose a range of costs on the individuals and organisations whose information has been exposed without authorisation. Some of those costs are directly financial, rather than in embarrassment, heightened risk of danger from stalkers and so forth

The Alerts Bill is deficient in terms of compliance. Penalties focus the mind wonderfully (and also gain the attention of journalists, thereby inducing greater awareness of breaches among managers and the community at large). On that basis the penalties for non-compliance with reporting requirements should not be trivial. Experience demonstrates that if they are trivial they will be disregarded, which negates the point of the proposed legislation. We should look beyond the Bill and ensure that privacy element of the Office of the Australian Information Commissioner has both the physical resources and the ethos to actively address compliance questions. In essence, there is no point in relying on a watchdog that is

underfed, lazy and too scared to leave its kennel.

Access

It is essential that, in implementing a breach reporting scheme and moving towards best practice, the community should have ready access on a timely basis to information about the breaches.

That information should not be 'hidden away' or buried. It should instead be readily accessible in a electronic form that is readily searchable and that is stable (ie does not disappear because of volatility in design and maintenance of a website). It should be incumbent on the Office of the Australian Information Commissioner to maintain and publish on a timely basis statistics about the breach regime. That may require additional staffing of the Office, an investment that is justified as a foundation of an effective regime that meets the needs of Australian consumers and that reinforces Australia's positioning in global e-commerce markets.

Yours sincerely

Bruce Arnold
Law School
University of Canberra

19 June 2013