20 June 2013 12:16 PM [email]

The Chair
Senate Legal and Constitutional Affairs Committee

Dear Senator Crossin

Re: Privacy Amendment (Privacy Alerts) Bill 2013

Thank you for the invitation to comment.

(Note that we received this at close of business Tuesday, due noon Thursday; the provision of around 10 working hours in which to collaborate on, draft and finalise a submission to your Committee is clearly inadequate, even given the demands of the legislative process.)

The submission from the Cyberspace Law and Policy Centre at UNSW on this Bill comprises only this message, and is necessarily incomplete. (We would normally hope to survey issues raised by others in some depth before focusing on particular aspects which deserver separate comment or support, but this has only happened in cursory form, as has the review of the text.)

Mandatory Data Breach Notification is increasingly the norm, and something we support in general: it has been law in parts of the USA for a decade, is increasingly common in other countries, and has been under discussion in Australia for years. The general concept is also increasingly accepted in Australia, including by some businesses who appreciate the transparency behind it as a necessary part of earning the essential ingredient, consumer trust and confidence in e-commerce and online systems in an environment where absolute security clearly can clearly not be promised.

A Mandatory Data Breach Notification scheme is not the answer to everything arising from a data breach, but is often helpful. And it is much better than accepting a silence, or a delay, after a breach, which some data hosts are tempted to do even with a voluntary scheme. The voluntary scheme which has been operating for several years has the potential for a perverse incentive to not disclose, since there are no real penalties, no clear obligations to breach, and notification is rarer and thus more likely to have a reputation impact as a novelty. To this extent it is more helpful to those not wishing to acknowledge a breach than those who accept their obligation as a matter of good practice.

A mandatory scheme by contrast creates the proper incentive to disclose, since there is a clearer obligation and potential penalties. Part of the benefit for business is that the more disclosures are notified, not only do consumers or data subjects get a better chance to respond and address their own interests quickly (the main purpose), but they also become more aware of the incidence of the problem, with attention then being

focused more on a.) the promptness and effectiveness of the notification and b.) other record-holder efforts to help mitigate the impact and avoid recurrence, rather novelty. The reputation risk (of being seen to behave inappropriately) is transferred to the non-discloser, who now stands out and is clearly not responding appropriately.

The Privacy Alerts Bill is however a 'lite' version of a Mandatory Data Breach Notification law.

Future international comparisons may show that, if passed in the current form, it will fall well short of best practice, and there may thus also be many Australians who might expect (and need!) to be notified under this model who may be still left in the current unsatisfactory limbo.

The Bill should be passed rather than rejected, but if passed should be substantially amended to address some of its shortcomings.

It is still worth noting that the title should use the by now conventional term ‘data breach notification’, so the Act should be called ‘Privacy Amendment (Data Breach Notifications) Act 2013’ or similar. This is a minor point, but puts it in the context of the growing international jurisprudence, and is not likely to have any deleterious effect on public awareness.

It is very important to cover offshore breaches under local control. To do otherwise is to invite offshoring to avoid the obligations, bad for consumers and bad for highly secure Australian online businesses. It is not clear that this is achieved.

The effect of a non-compliance with notification obligations should be treated similarly to other breaches of privacy. A breach of the compliance obligation should clearly constitute an 'interference with privacy' to enable access to other capabilities and regulatory responses if necessary, including civil penalties in the worst cases. It appears that this treatment has been taken into account in this version of the Bill in s3 which creates a new s13A in PA; this is a very welcome development.

It is equally important to limit the scope for exceptions and excuses, for non-disclosure where there is any prospect of impact on subjects. This aspect is deficient as the scope is limited to only those entities covered by the Privacy Act, which is too narrow. The Bill should cover all organisations and all data types of "personal information" that could be subject to a data breach and be covered by the Commonwealth's powers. Many new e-commerce entities will be exempt, yet they can do serious damage with poor practice, and need to be held to the same protective standard to avoid undermining public confidence in ecommerce data safety.

Exceptions, if they are permitted, should be limited to named entities not classes, require full justification and verification, be limited in duration to the minimum time necessary, not allow failure to inform the regulator, and otherwise be as limited as

possible. (Past practice with privacy amendments has been to include a raft of such exceptions, undermining the main provisions; in the case of data security, it is too important to offer an easy excuse for non-compliance.) Similarly, the OAIC's operation of the scheme should not be subject to discretionary variation or exceptions; where discretions exist they should be defined, and transparently reported. This Bill should not set up a scheme were there is an endless queue to the commissioner's door for secret exemptions, which would undermine the purpose of the Bill, and the basis of public trust and confidence that they will be able to find out if there is a breach; this would be both a waste of the commissioner's time, which is better spent pursuing breaches and complaints, and undermines the expectation of compliance.

Equally, the type of potential harm needed to trigger an obligation should be more broadly cast, to also include e.g. serious inconvenience or need for very onerous action not limited to pure financial costs, impact on capacity to get services like credit, housing, insurance etc, and serious mental harm or distress.

Public access to information on both statistics (by sector and over time) and individual case details is very useful. This can be achieved quite cheaply with modern online tools. The benefit outweighs the cost here. It should be mandated.

We would expect an explicit obligation on the regulatory system to either itself publish or require publication of both case details and statistics in an efficient, searchable public online register, with stats and serious breaches published online permanently. (Too much online material about the operation of the law in this area is at risk of being lost due to the folly of unpublishing documents during bureaucratic reorganisations and administrative changes, so the permanency should be explicit.)

The Privacy Commissioner should be expected to issue supplementary guidelines setting out suggestions for good practice in more detail.

yours sincerely

David Vaile, Alana Maurushat and Lyria Bennett Moses
for Cyberspace Law and Policy Centre,
UNSW Faculty of Law