005ASubmission to the Serious Data Breach Notification Consultation

(Consultation closes 4 March 2016 — please send electronic submissions to privacy.consultation@ag.gov.au)

Your details

Name/organisation *(if you are providing a submission on behalf of an organisation, please provide the name of a contact person)*	Mr Philip Green Privacy Commissioner Office of the Information Commissioner Queensland
Contact details *(one or all of the following: postal address, email address or phone number)*	PO Box 10143 Adelaide Street Brisbane QLD 4000 Telephone: (07) 3405 1111 Fax: (07) 3405 1122 Email: administration@oic.qld.gov.au

Publication of submissions

In meeting the Australian Government's commitment to enhancing the accessibility of published material, the Attorney-General's Department will only publish submissions to this website that have been submitted electronically.

Our preference is that submitters complete this template and send it to privacy.consultation@ag.gov.au.

However, if submitters choose to provide a separate document, the following formats are preferred:

- Microsoft Word
- Rich Text Format (RTF)
- txt format.

Please limit individual file size to less than 5MB. The department may create PDF documents from the above formats.

The department will still consider hardcopy submissions received by mail, but these submissions will not be published on the website.

Confidentiality

Submissions received may be made public on the Attorney-General's Department website unless otherwise specified. Submitters should indicate whether any part of the content should not be disclosed to the public. Where confidentiality is requested, submitters are encouraged to provide a public version that can be made available.

Would you prefer this submission to remain confidential? NO

Your submission

The Queensland Office of the Information Commissioner is an independent statutory authority. This submission does not represent the views or opinions of the Queensland Government.

The statutory functions of the Information Commissioner under the *Information Privacy Act 2009* (Qld) (**IP Act**) include commenting on issues relating to the administration of privacy in the public sector environment.

The Office of the Information Commissioner (OIC) generally supports measures strengthening protections against abuses of privacy, particularly where inadequacies with the existing regulatory framework are identified. In principle, OIC supports the introduction of a statutory mandatory breach notification scheme.

The rapid growth in the commoditisation of 'personal information', and the increasingly sophisticated methods by which personal information can be obtained, used and disseminated expose individuals to new privacy risks and exacerbate existing risks. The OIC considers the introduction of a mandatory data breach notification scheme strengthens the existing regulatory framework and brings Australia in line with other jurisdictions, including the EU, the United Kingdom and the United States.

Queensland privacy law

On 1 July 2009, Queensland enacted the *Information Privacy Act 2009* (**IP Act**). The IP Act regulates how government agencies collect, store, use and disclose 'personal information' through obligations to comply with 'privacy principles' consisting of:

- Information Privacy Principles (**IPPs**) – for all government agencies other than Health Agencies;[1] or
- National Privacy Principles (**NPP**s) – for Health Agencies;
- provisions dealing with service providers contracted to government agencies; and

[1] A health agency is the Health Department or a Hospital and Health Service.

- provisions dealing with the transfer of personal information outside Australia.

Queensland's IP Act only applies to Queensland State Government agencies which include Ministers, Queensland State Government Departments, Local Government and Public Authorities (agencies).[2] The IP Act does not apply to Government Owned Corporations (**GOCs**), individuals, the private sector or community organisations unless a contracted service provider is contractually bound to comply with the privacy principles. Queensland GOCs, the private and community sector could be covered under the Commonwealth's privacy legislation if these entities have an annual turnover of more than $3 million per annum.

Data breach notification obligations in Queensland

Queensland's privacy principles include obligations which require agencies and bound contracted service providers to protect the personal information they hold from misuse, loss, and from unauthorised access, modification or disclosure. The IP Act also obliges agencies to safeguard the privacy of personal information when transferring personal information outside of Australia.

However, the IP Act does not require agencies to notify either affected individuals or the Information Commissioner of a privacy breach.

Queensland State Government agencies have obligations to report information security incidents to the Queensland Government Chief Information Officer as part of the IS18 information security incident reporting requirements.

OIC encourages agencies under the IP Act to incorporate data breach notification into its information management processes as a responsible business practice. OIC also encourages agencies to communicate with the Queensland Commissioner when incidents of data breach occur. OIC can provide guidance and information concerning privacy breach management, and OIC can be used as a sounding board concerning when potential notification of individuals may be appropriate. OIC has produced a 'Privacy breach management and notification guideline'[3] which provides written guidance for agencies considering notification.

To date, only a small number of Queensland State Government agencies and their contracted service providers have reported data breach notifications to the OIC. One possible explanation for the relatively low number is that data breach is a relatively rare occurrence in Queensland. However, in the absence of reliable data and a legislative framework mandating reporting of data

[2] IP Act also applies to contractually bound contracted service providers
[3] http://www.oic.qld.gov.au/information-and-resources/guidelines/guidelines-privacy-principles/privacy-breach-management

breaches, it is difficult to state with any certainty the actual numbers of data breaches in Queensland.

The introduction of mandatory data breach notification for those entities currently subject to the *Privacy Act 1988* (Cth) is unlikely to have any direct impact on those agencies subject to OIC's jurisdiction. However, OIC's view is that introduction of mandatory data breach notification sets an important precedent for State and Territory legislation. OIC offers the following comments on the draft Commonwealth *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015* (**draft Bill**).

Mandatory data breach notification scheme

OIC supports the introduction of a legislated mandatory data breach notification scheme by the Commonwealth Government.

OIC concurs that the primary rationale for mandatory data breach notification is to allow individuals whose personal information has been compromised in a data breach to take remedial steps to lessen the adverse impact that might arise from the breach, such as financial loss or identity theft.

For governments particularly, mandatory data breach notification is an important transparency measure. Governments collect and hold vast amounts of personal information on behalf of its citizens and citizens trust that Governments will protect this information from unauthorised access, use and disclosure. Increasingly, this information is held electronically posing significant implications for an individual's privacy in the event of a data breach. As noted by the OECD, trust in institutions including government continues to decline and only 40% of citizens trust their government.[4] Openness and transparency is an important mechanism for building trust and confidence in government.

A mandated scheme for the notification of data breaches increases the public's confidence that they will be made aware if their personal information is compromised. It also signifies to the public the importance government attaches to its information security practices and the protection of an individual's personal information.

Mandatory data breach notification also ensures that the public are not unnecessarily placed at risk by a failure to notify. Given the significant economic and reputational costs associated with

[4] Organisation for Economic Development (OECD), Trust in Government, http://www.oecd.org/gov/trust-in-government.htm

data breaches, mandating notification can be an effective tool to require entities to improve their privacy, data handling and data security practices.

While OIC acknowledges that these protections are limited to entities currently covered under the Commonwealth's Privacy Act, the precedent value of this development remains. Also, to date significant privacy breaches have occurred in industries that have corporations that would be covered under this scheme and which hold considerable stores of personal information – banking and finance, telecommunications and entertainment.

OIC notes the draft Bill provides limited exceptions to the data breach notification requirement including:

- law enforcement activities are likely to be prejudiced;
- notification is inconsistent with another law of the Commonwealth that regulates disclosure of information;
- the Australian Information Commissioner exempts an entity from providing notification, on its own initiative or on an application from an entity, if satisfied it is in the public interest to do so; and
- the entity carries out an assessment within the required timeframe and finds there are not reasonable grounds to believe a serious data breach has occurred.

OIC supports the flexibility provided by the draft Bill, including the nature of the exceptions, regarding the obligation to notify data breaches.

Notification Threshold

OIC notes that the draft Bill will require entities to notify the Australian Information Commissioner and affected individuals in the event of a 'serious data breach', subject to limited exceptions, which is defined as unauthorised access to, or disclosure/loss of, personal information, credit reporting information, credit eligibility information, or tax file number information that puts the individual or individuals at '*real risk of serious harm*'. The Explanatory memorandum notes that the notification threshold is based on the standard recommended by the ALRC and incorporated in the current voluntary data breach guidelines issued by Australian Information Commissioner.

As noted in the *Discussion Paper: mandatory data breach notification* (**Discussion Paper)** accompanying the draft Bill, the proposed Australian mandatory data breach notification scheme has a relatively higher notification threshold in comparison to similar schemes in other jurisdictions. The stated rationale for setting a higher notification threshold is to 'avoid the risk of

'notification fatigue and unnecessary administrative costs for businesses'. The Explanatory memorandum notes that 'it is not intended that every data breach be subject to a notification'.

OIC acknowledges the difficulties in striking the appropriate balance between increasing the regulatory burden on businesses and protecting the public's privacy. Implementing a legislative framework to require reporting of all data breaches may not be practicable or feasible particularly in circumstances where notification is unlikely to lessen the harm resulting from the breach. In some instances, depending on the nature of the breach, notification may actually exacerbate the impact of the breach. However, setting the threshold for notification too high may have a number of implications for entities, including government agencies, and individuals affected by a data breach.

Data breaches that do not reach the threshold for notification under the draft Bill are unlikely to be voluntarily notified by entities given the significant financial and reputational costs once a data breach has been made public. Setting a high notification threshold may result in only the most egregious of breaches being notified.

Monitoring and reporting of all data breaches allows important information about an entity's privacy and data security practices to be analysed which may lead to the identification of broader systemic problems. In the absence of reliable data and information about the prevalence and nature of data breaches, it is difficult for entities to implement strategies to address existing deficiencies in their existing privacy and data security practices to prevent data breaches occurring in the future.

As noted in a report about cyber security by Chartered Accountants Australia and New Zealand, 'organisations feel immune from attack because of the lack of cyber-crime statistics… and limited regulatory options with which to penalise organisations. The lack of data and threat of penalty means that cyber security is often way down the boardroom agenda, and worse, is often ignored altogether'.[5]

For individuals, a lack of information and awareness about a data breach impedes the individual's ability to take whatever action the individual deems appropriate in their particular circumstances, irrespective of the extent of the harm caused. A key tenet of privacy is that individuals should be afforded choices and be able to exercise control in respect of their own information as far as possible.

To ensure that data breaches which do not meet the threshold for notification are addressed, consideration could be given to placing an obligation on entities, in particular government

[5] *Protecting our Cyber Future*, Future inc, Chartered Accountants Australia and New Zealand, http://charteredaccountantsanz.com p6

agencies, to record instances when an individual's privacy is potentially compromised by a data breach. This information could then be reported on an annual basis to Australian Information Commissioner.

OIC welcomes provisions in the Bill that provide for regulations to specify particular situations that may also be serious data breaches even if they do not necessarily reach the threshold of a *real risk of serious harm.* While no specific categories have been prescribed to date, the explanatory memorandum notes this could include the release of particularly sensitive information such as health records which may not cause serious harm in every circumstance but should be subject to the highest level of privacy protection.

Timing of Notification

The draft bill provides that the regulated entity must notify the Australian Information Commissioner and affected individuals 'as soon as practicable' after the entity is aware, or ought reasonably to have been aware, that there are reasonable grounds to be believe that there has been a serious data breach.

The draft bill also provides that where an entity suspects but is not certain that a serious data breach has occurred, the entity has up to 30 days to assess whether there are reasonable grounds to believe that a serious data breach has occurred. If the entity assesses there has been no serious data breach, notification is not required.

OIC considers timely notification of a breach is vital. OIC acknowledges that due to the increasingly sophisticated nature of data breaches, determination of whether or not a notifiable data breach has occurred can be complex and may not be immediately obvious.

However, failure to notify an affected individual within the outer limits of the 30-day time period may negatively impact on an individual's ability to take appropriate action to mitigate any damage arising from the breach, particularly if the entity subsequently determines a notifiable breach has occurred.