COMMUNICATIONS
ALLIANCE LTD

# COMMUNICATIONS ALLIANCE

## Submission to the Attorney-General's Department in response to the Exposure Draft of the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015

March 2016

Communications Alliance welcomes the opportunity to provide the Attorney-General's Department with a submission in response to the Exposure Draft of the *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015* and any associated material.

## ABOUT COMMUNICATIONS ALLIANCE

Communications Alliance is the primary telecommunications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to provide a unified voice for the telecommunications industry and to lead it into the next generation of converging networks, technologies and services. The prime mission of Communications Alliance is to promote the growth of the Australian communications industry and the protection of consumer interests by fostering the highest standards of business ethics and behaviour through industry self-governance. For more details about Communications Alliance, see http://www.commsalliance.com.au.

# 1. INTRODUCTION

Through the accelerating digitisation of economic and service delivery frameworks in Australia and across the globe, the amount of data relating to individuals and societies in general being held by commercial entities and Government agencies has exploded during the past decade.

The continuously improving ability to interrogate databases (often close to or in real-time) and to combine fragments of data into a larger picture that can identify individuals or groups, means that data has become a potent resource which must be protected to ensure the privacy of individuals.

To comply with the mandatory data retention regime introduced in Australia in 2015 large additional volumes of often personal data must be retained and stored by telecommunications providers.

Industry is acutely aware of the need to protect any data it collects and/or holds as a result of 'ordinary' operational or regulatory and legal requirements such as the data retention regime. Industry has a strong vested interest in ensuring that such data is protected from unauthorised access, disclosure, interference or loss. Consequently, Industry is commercially motivated to make very large investments in the protection of data, including through the hardening and protection of networks and communications infrastructure from external attack. Industry also has a proven track record of close and effective cooperation with Government agencies (and each other within the confines of the law) to ensure there is shared understanding of any potential threats and coordinated action at all levels.

Industry acknowledges that despite its best efforts, absolute protection of data, including personal data, will not always be possible and data may be accessed or disclosed in an unauthorised manner or lost, i.e. data breaches may occur. Accordingly, Industry recognises the need for a mechanism by which individuals affected by the data breach must be notified in order to alert them to the potential compromise of their privacy and to minimise the potentially negative consequences of such a breach.

Communications Alliance welcomes the Exposure Draft of the *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015* (Exposure Draft) as an improvement on drafts and concepts that have been discussed in the past. However, Industry believes that the Exposure Draft requires further work to create a more practicable and effective notification mechanism that provides sufficient clarity to Industry and avoids 'notification fatigue' for affected individuals.

In the following, we highlight some areas of concern with the current Exposure Draft.

# 2. CONCERNS AND SUGGESTED IMPROVEMENTS

### DATA MEDIUM

Industry assumes that the draft legislation applies to all data within the defined scope regardless of the medium being used to hold the data, e.g. paper or electronic.

Consideration ought to be given to limiting the legislation only to computerised data as it is the case for most US data breach notification laws.

### TITLE AND USE OF THE TERM 'SERIOUS DATA BREACH'

The title of the Exposure Draft as well as the text throughout the draft legislation refer to a notifiable breach as a 'serious data breach'. While Industry does not in any way wish to dispute that data breaches can indeed be very serious, it may be more useful to refer to the breaches under consideration as 'notifiable data breach' or similar.

When notifying affected individuals, entities are likely to reference the underlying legislation and the inclusion of 'serious' in the title and throughout the legislation might lead to unnecessary 'panic' with the affected individuals.

Using the term 'notifiable breach' also more closely reflects the actual logic implied in the draft legislation, i.e. when a breach has occurred that carries a 'real risk of serious harm' (noting that it remains a 'risk' as opposed to a fact that harm actually does occur), then that breach has to be notified. This means that the harm may be serious but the breach as such should be labelled 'notifiable'.

Importantly, also note Industry's concerns around the subjectivity of the word 'serious' in 'serious harm' discussed further below.

## RISK OF MULTIPLE NOTIFICATIONS FOR THE SAME BREACH

The proposed legislation applies to entities that 'hold' personal information or certain other kinds of information with 'hold' being defined in Section 6(1) of the *Privacy Act 1988* (Privacy Act) as "hav(ing) possession or control of a record that contains the personal information". The Office of the Australian Information Commissioner's *Australian Privacy Principles Guidelines* state that "the term 'holds' extends beyond physical possession of a record to include a record that an APP entity has the right or power to deal with. For example, an entity that outsources the storage of personal information to a third party, but retains the right to deal with that information, including to access and amend it, holds that personal information."

As the example above already demonstrates, it is very likely that the same data is 'held' by several entities involved in the supply chain for the provision of telecommunications services, e.g. a carriage service provider ('holder' 1) may disclose customer data to an outsourced call centre provider ('holder' 2), who outsources storage of some of the data to a third party ('holder' 3). Alternatively, an entity may host a third party business customer's client data as part of its cloud product, i.e. the data under consideration is being 'held' by two parties. The above means that every 'holding' entity is required to separately notify any affected individual about a single breach (provided that the breach is notifiable).

It is likely that affected individuals (and potentially also the Australian Information Commissioner (Commissioner)) would not be aware that the notifications that they receive relate to the same data breach. Even if they did realise, receipt of multiple notifications within a short timeframe bears the risk of leading to 'notification fatigue' and, as a result, affected individuals may no longer take the recommended steps to limit any detrimental impact on their privacy that the breach may have.

Industry, therefore, favours a mechanism that ensures that only one entity will notify a breach. A distinction similar to the distinction of 'data controller' and 'data processor' in the *Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*[1] (GDPR) might be useful. Article 4 of the GDPR defines 'data controllers' as the body "which alone or jointly with others determines the purposes, conditions and means of the processing of personal data". Meanwhile, the 'processor' is the body "which processes personal data on behalf of the controller". The GDPR establishes a chain of notification: where a notifiable data breach has occurred, Article 31.2 of the GDPR requires 'processors' alert 'controllers' of such breach but not more. 'Controllers', meanwhile, are obliged to notify the relevant authorities and affected individuals about a breach (GDPR, Article 31.1).

Similarly, US state data breach notification laws delineate between companies that own or license data vs entities that maintain information on behalf of these data owners. The distinction is similar to the GDPR 'data controller' vs 'data processor' approach. Under US

[1] Refer to http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf for a copy of the legislation

laws, the data owner must notify affected individuals and state agencies while third parties must notify the data owner. Importantly, data owners can contractually require third parties to notify affected individuals.

The Australian draft legislation does not currently offer this separation of status for different entities along the chain of information control and processing and is likely to result in the aforementioned inefficiencies. It ought to be amended to avoid multiple notifications.

**NOTIFICATION THRESHOLD**

**Definition of threshold:**

A data breach must meet two threshold tests in order to be notifiable – it must have the potential to cause 'serious harm' and the risk of doing so must be 'real'.

***'real risk':***

Section 26WG of the Exposure Draft defines 'real risk' as "a risk that is not a remote risk". Unfortunately, this definition does little to assist Industry to assess whether the risk is 'big enough' to meet the threshold.

Therefore, Industry recommends the use of more commonly known terms which lend themselves better to some form of statistical test, e.g. use of the terms '(im)probable' or '(un)likely'.

Such an approach would also be in line with Article 31(1) of the GDPR which uses 'unlikely' (to result in "a high risk for the rights and freedoms of individuals") as the threshold.

***'serious harm':***

The second threshold test of the breach resulting in 'serious harm' (assuming the risk test has been satisfied) raises concerns on two levels:

*'serious':* the term 'serious' is not defined in the draft legislation. The definition of 'serious' in the Macquarie dictionary includes "giving cause for apprehension" or "give rise to fear or anxiety", thereby introducing a subjective element (one person may be apprehensive when another sees no reason to feel that way) into the key threshold test for notification. It would be preferable to use a more legally tested term, such as 'material'.

*'harm':* the Exposure Draft includes 'emotional' and 'psychological' harm in its definition of 'harm'. Industry strongly objects to this incredibly large scope of harm and requests the removal of those terms from the definition. Whether 'serious' (or 'material' as suggested above) 'emotional' harm has occurred would be entirely dependent on the level of fortitude of the affected individual or even on the assessment of what constitutes an emotion. The current definition would essentially mean that entities would have to notify in almost all instances of data breach (assuming 'real risk') as a reasonable assessment of 'emotional' and 'psychological harm' is impossible, particularly where large numbers of unknown individuals are concerned.

**Assessment of meeting the threshold:**

Industry also considers that the notification threshold for affected individuals ought to be assessed separately from the threshold for notification to the Commissioner. Both could retain the 'real risk of serious harm' test but the notification to the Commissioner could include an additional materiality threshold, possibly based on the number of individuals affected (similar to the US scheme[2]) and/or be based on the nature of the incident (e.g. malicious vs accidental) and/or whether such notification is in the public interest.

By separating the two assessments it would be possible to assess notifications to affected individuals or a subset thereof on a case by case basis, and assess notifications to the Commissioner only if both the harm and materiality threshold have been reached. The suggested separation of the two assessments could be accompanied by a requirement for

[2] Sec. 103, The Personal Data Notification & Protection Act

an entity to maintain a 'breach register' to record breaches and the entity's 'justification' and conclusion as to whether or not to notify the Commissioner, as well as powers for the Commissioner to audit an entity's register.

This approach would reduce the administrative burden for Industry and Government alike while also better reflecting the practicalities of notifications. The Australian Securities and Investment Commission (ASIC) approach for *Breach Reporting by AFS Licensees*[3] may serve as a practical in-market example.

**Notification of individuals who meet the threshold test:**

Moreover, it appears that once the threshold for notification has been met on the basis of a 'real risk of serious harm' for *one* individual, the draft legislation requires an entity to notify all individuals subject to that data breach even if the 'real risk of serious harm' threshold has not been met for the other individuals subject to the notifiable data breach. Industry recommends that the Exposure Draft is amended to ensure that the notification requirement is limited to individuals for which the 'real risk of serious harm' threshold has been met. This will reduce the likelihood of 'notification fatigue' where individuals are being notified in circumstances where there is no 'real risk of serious harm'.

## MITIGATION OF RISK

The Exposure Draft appears to offer a form of a mitigation mechanism. However, the workings of this mechanism – and the fact that, upon positive assessment, it grants an exemption from notification – ought to be stated more explicitly.

Section 26WB(3)(i) allows entities, as part of determining whether there is a 'real risk of serious harm', to "have regard" to the nature, speed and effectiveness (actual or predicted) of mitigating measures (whether completed, currently pursued or to be pursued in future).

It appears that, where an entity reasonably believes that the mitigating measures it has taken do indeed negate the 'real risk of serious harm', then a notification would not be required by virtue of no longer meeting the notification threshold. However, an express connection of mitigating measures and the notification requirement – or rather the fact that notification would no longer be required in such a case – would be desirable.

In this context, please also refer to our comments with regard to encryption (as a potentially mitigating measure) further below.

## NOTIFICATION TIMEFRAME AND TIMING

Section 26WC(2) of the Exposure Draft requires entities to conduct a reasonable assessment of whether a notifiable data breach has occurred "as soon as practicable" but in any case within 30 days of the entity becoming aware (or when it ought to have become aware) that the breach has occurred. Industry notes that an assessment of the circumstances involving a data breach can be very complex and may take longer than 30 days to complete. A mechanism to request an extension (by say another 60 days) – and the possibility of appealing a negative decision – for complex assessments ought to be included into the legislation.

The draft legislation ought also to be amended to make it clear that in cases where an entity finds, after assessment of a breach, that there is no 'real risk of serious harm' but alters its view at a later point due to new, previously unknown information, the 30 day period commences from awareness of the new information rather than from awareness of the data breach.

Industry also seeks clarity with regards to the order of notifications to affected individuals and to the Commissioner. It appears that there may be an implicit assumption that notification to the Commissioner precedes notification to affected individuals (as the Commissioner has the

[3] See http://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-78-breach-reporting-by-afs-licensees/

power to direct entities to notify individuals) but the legislation itself ought to provide clarity on this issue.

## 'ORDINARY PERSON' AND ENCRYPTION

Sections 26WB(3)(c) and (d) of the draft legislation require entities, as part of determining whether there is a 'real risk of serious harm', to "have regard to (...) whether the information is in a form that is intelligible to an ordinary person" and "if the information is not in a form that is intelligible to an ordinary person – the likelihood that the information could be converted into such a form".

While Industry appreciates the concept underlying the current draft legislation, we note that a practicable application, as envisaged and described in the Explanatory Memorandum, would be difficult or impossible to achieve.

The Explanatory Memorandum indeed seems to contradict the concept of 'ordinary person' by stating that "The test is not intended to preclude consideration of whether the information would be intelligible to a person with knowledge or capabilities exceeding those of an ordinary person (...)"[4] and by referencing the "sophisticated attacker" who may be able to break encryption algorithms. In addition, the Explanatory Memorandum introduces a time component, i.e. whether or not such cracking of an encryption algorithm may occur in the long-term.[5]

Industry contends that the above would essentially result in almost all data breaches being notifiable as the entities suffering the data breach may not have knowledge of who gained access to the data and, even where it did have this knowledge, the likelihood that data could (note not necessarily *would*) be made intelligible, now or in the long-term, always seems to be reasonably high, particularly where the 'sophisticated attacker' is concerned.

It is also not clear how the above concept, and particularly the examples provided in the Explanatory Memorandum, relate to Section 26WB(3)(e) which stipulates "protec(tion) by one or more security measures" – and one would think that encryption would be counted as such a measure – as an issue to have regard to when making the assessment of 'real risk of serious harm'.

The GDPR takes a more pragmatic approach by exempting the entity from notifying the affected individual if it "has implemented appropriate technological and organisational protection measures and those measures were applied to the data affected by the personal data breach, in particular those that render the data unintelligible to any person who is not authorised to access it, such as encryption". This approach allows entities to make a much more straight forward assessment of whether there is a 'real risk of serious harm' and it is recommended for adoption in the Australian context. (If adopted, it should be noted that Industry by no means wishes to state that any breach of non-encrypted data would, *by definition*, carry a 'real risk of serious harm'.)

## INFORMATION SPECIFIED IN REGULATIONS

Sections 26WB(2)(ii) and (c)(ii) of the Exposure Draft work to create a 'serious data breach' where "information (...) of a kind specified in the regulations" is subject to unauthorised access, unauthorised disclosure or loss without invoking the 'real risk of serious harm' test. Industry seeks clarity what circumstances could arise to warrant these regulations. It appears that the authors of the draft legislation may already have some kinds of data in mind which may be subject to regulations and, consequently, Industry would like to engage in early discussions to gain a better understanding of what is being expected of them. Consideration also ought to be given to introducing a test for notification for these kinds of data breaches.

[4] p.15, items 44ff, Explanatory Memorandum to the *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015*

[5] p.15, item 45, Explanatory Memorandum to the *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015*

Industry also suggests that the data breaches to which the regulation could apply be limited to 'sensitive' information (as defined in the Privacy Act) or categories of 'sensitive' information.

**COMMISSIONER'S MANDATING POWERS**

The Commissioner has the power to direct entities to notify affected individuals if he believes, on "reasonable grounds", that a serious data breach has occurred (Section 26WD(1)). Section 26WD(5) requires entities to comply with such a direction "as soon as practicable after the direction is given". This provides the Commissioner with the power to require reporting without the accompanying requirement of consultation and providing a right of reply to the entity. The Commissioner should also be obliged to provide full details of the alleged breach in circumstances in which the entity is not aware of the facts.

Also, neither the Exposure Draft nor the Explanatory Memorandum provide any clarity on what timeframe 'as soon as practicable' may involve. An entity's assessment of a data breach incident is often conducted under time pressure with limited information and the Commissioner's powers in these circumstances ought to reflect these competing demands. Industry notes that sufficient time for investigation of an alleged breach (i.e. timeframes equivalent to those that would apply had the entity found the serious data breach by itself) will be required to allow efficient notification of affected individuals and, where appropriate, to explore options for appeal against the direction.

**COMMISSIONER'S EXEMPTION POWERS AND DEFAULT EXCEPTIONS**

Sections 26WC(6) and (7) of the draft legislation grant powers to the Commissioner to exempt an entity from its notification requirements. However the Commissioner is only allowed to do so if he is satisfied that it is in the 'public interest' to grant such exemption.

Industry believes that the test for the Commissioner granting an exemption ought to be wider than the 'public interest', e.g. whether the notification could cause serious harm to the notifying entity or cause the notifying entity to breach security obligations ought to be taken into account when determining whether an exemption could be justified. Therefore, Industry recommends a 'reasonability test' combined with a mandatory regard to the 'public interest'.

It is also suggested to include certain financial services related grounds into the test for granting exemptions, e.g. in

- Instances of fraud where information is released to a person who fraudulently obtains identification details of another person.
- Individual instances of fraud where financial institutions ultimately bear the financial risk, not the individual.
- Systemic instances of fraud where financial institutions are the primary target and who ultimately bear the financial risk, and with whom the data breach notification obligations ought to rest.

We also note that Section 26WC(5)(b) creates notification exceptions (not *exemptions*) for enforcement bodies where the "enforcement body believes on reasonable grounds that compliance with those paragraphs would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, the enforcement body". It appears that this is a relatively low threshold for enforcement bodies and it is not clear why the law would not work to equally apply to enforcement bodies with a requirement to notify the affected individuals unless the Commissioner decides on 'reasonable grounds' to exempt the enforcement body (in that instance) from the notification requirement.

**ENFORCEMENT/PENALTIES**

Section 13(4)(A) of the Exposure Draft provides that a contravention of Section 26WC or 26WC is deemed an "interference with the privacy of an individual" thereby making a failure

to comply subject to a civil penalty under Section 13G of the Privacy Act (with a maximum of 2000 penalty units, i.e. $360,000 ($1.8M for body corporates)).

Industry suggests that, when determining the application of penalty provisions, consideration ought to be given as to what steps an entity has undertaken to remedy a data breach.

# 3. CONCLUSION

Industry appreciates the engagement in the process so far and is hoping to continue to engage with the Attorney-General's Department and Parliamentary Committees. We would be very happy to review a second exposure draft to ensure that a mandatory data breach notification scheme in Australia can be a useful and efficient tool to address data breaches in an ever increasing digital environment.

For any questions relating to this submission please contact Christiane Gillespie-Jones on 02 9959 9118 or at c.gillespiejones@commsalliance.com.au.

COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507