18 June 2021

NSW Department of Communities and Justice
By email: policy@justice.nsw.gov.au

Submission to Inquiry into Privacy and Personal Information Protection Amendment Bill 2021

About us

The Allens Hub for Technology, Law and Innovation ('the Allens Hub') is an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law, the Allens Hub aims to add depth to research on the diverse interactions among technology, law, and society. The partnership enriches academic and policy debates and drives considered reform of law and practice through engagement with the legal profession, the judiciary, government, industry, civil society and the broader community. More information about the Allens Hub can be found at http://www.allenshub.unsw.edu.au/.

The Australian Human Rights Institute breaks silos between academic research and real-world problems to progress human rights. The Institute builds on the outstanding legacy of the Australian Human Rights Centre which, since its establishment in 1986, has increased public awareness and academic scholarship on human rights through research, public lectures and events, and publications. The Institute deliver multidisciplinary, applied research, empowering communities and educating the next generation of human rights leaders. It works in partnership with government, industry and human rights defenders through advocacy, education and public engagement to achieve impact. More information about AHRI can be found at https://www.humanrights.unsw.edu.au/

The ARC Centre of Excellence for Automated Decision-Making and Society brings together universities, industry, government and the community to support the development of responsible, ethical and inclusive automated decision-making. The Centre combines leading researchers from the humanities, social and technological sciences in an international industry, research and civil society network. It work with technologists, policy-makers, and public communicators, and aims to enhance public understanding, inform public debate, and train a new generation of researchers and practitioners in the challenging new field. More information can be found at: https://www.admscentre.org.au/.

About this Submission

Our submission focuses on aspects of the Bill on which our research can shed light. We thus limit our submission to:

1. reasons why we support a Mandatory Notification of Data Breach Scheme (MNDB scheme);

2. a suggestion for reframing the "serious harm" threshold in the definition of "eligible" data breach;
3. a suggestion to incorporate reflection on the extent to which encryption is protective in section 59G(c); and
4. a suggestion to remove "date of birth" from section 59Q(1).

Our submissions reflect our views as researchers and is not an institutional position of UNSW Sydney, Allens or any other organisation.

Support and need for mandatory data breach notification scheme

An MNDB scheme fulfils several important functions, including:[1]

1. It empowers data subjects at risk as a result of a data breach to take self-protective measures. This is important in general, but may be particularly significant in a context (1) of family and/or domestic violence, (2) where those affected are encouraged to take specific precautionary measures such as changing passwords, notifying financial service providers, or remaining wary of potential social engineering attempts.
2. It enhances trust in those agencies participating in the scheme; data subjects know that they will be notified should they be at risk of serious harm as a result of a data breach.
3. It increases information sharing about breaches among the cyber security community. This is because it reduces the reputational cost of sharing information given the pre-existing publicity associated with disclosures under the scheme. Sharing information about data breaches can improve cyber security both within government and beyond.
4. It encourages improved cyber security practices generally due to the consciousness of reputational risk should a breach occur. This may also lead organisations to delete data when no longer required.
5. It creates consistency between the NSW and Commonwealth legislation, including in relation to accessed and retained telecommunications data.
6. It reduces the risk associated with data breaches, which is otherwise increasing with ever larger amounts of data processed by the NSW government.

Scope and Seriousness of data breaches under the scheme

The Bill will insert section 59C into the *Privacy and Personal Information Protection Act 1988*, which sets the standard for eligible data breaches as those involving "serious harm to an individual to whom the information relates". This mirrors the scope of the Commonwealth scheme. While there are advantages in uniformity, we believe the standard is problematic because:

[1] Many of these points were made in Genna Churches, Monika Zalnieriute and Graham Greenleaf, *NSW Needs a Strong Mandatory Data Breach Scheme: Submission to Inquiry into NSW Adopting a Mandatory Reporting Scheme for Data Breaches* (Submission, The Allens Hub, 23 August 2019) 1.

1. a responsible agency deciding whether the "serious harm" test is met may not be aware of the particular situation of the individual (for example, whether they are concerned about violence from a former intimate relationship) and thus may reach inaccurate conclusions;
2. it is possible that, in making the assessment, an agency will not be aware of other available data which might compound the risk to individuals (for example, by facilitating re-identification of publicly available de-identified information about individuals or by forming a crucial part of a mosaic of information about an individual);
3. such high threshold does not reflect the expectation of the public who are concerned with breaches of privacy (and not only 'serious harm');
4. such high threshold is not in line international standards such as those under the *General Data Protection Regulation* ('*GDPR*').[2]

Thus, we suggest that the threshold in s 59C be replaced with something analogous to a reversed onus. This allows for the same standard across jurisdictions ("serious harm") but requires notification unless a particular public sector Department can demonstrate that there is *no* serious harm. In particular, the NSW Privacy Commissioner and affected individuals should be notified unless an agency can demonstrate that the breach is *unlikely* to result in serious harm, including to an individual's human rights as recognised in international law. As Churches, Zalnieriute and Greenleaf elaborated in Section 3 of their earlier submission,[3] this is similar to the standard in the *GDPR.* There, reporting is mandated *unless* the risk to individual's rights is *unlikely*.[4] The modified scope would not be inconsistent with Commonwealth legislation, but would place NSW at the forefront among Australian jurisdictions of international best practice.

Section 59G(c)

The factor ought not to be *whether* security measures are used but rather the sufficiency of those measures in the context of an existing breach. For example, if encryption were used, the next question should be to assess the computer resources required to brute force decryption within the timeframe in which harm might be caused. We suggest supplementing the end of the sentence by adding "and, if so, the likelihood that they will protect individuals to whom information relates from serious harm."

Section 59Q(1)

It is not clear why information about 'date of birth' is necessary to inform an individual of the fact of a data breach. Indeed, this information is itself sensitive and is sometimes used as a proxy identifier (in that some organisations use it to verify an individual is who they say they are). That might be bad

[2] Articles 33 and 34 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88 ('*GDPR*').
[3] Churches, Zalnieriute and Greenleaf (n 2).
[4] *GDPR* arts 33, 34.

cyber security practice, but it is nevertheless pervasive. Name and contact details and, where relevant, fact of death, ought to be sufficient to administer the notification scheme.

Yours sincerely,

[redacted]