Submission No 18

INQUIRY INTO CYBERSECURITY

Organisation: Office of the Australian Information Commissioner

Date Received: 21 September 2020

Australian Government
Office of the Australian Information Commissioner

Our reference: D2020/017624

The Hon Tara Moriarty MLC
Committee Chair
Portfolio Committee No. 1 – Premier and Finance
Parliament House, Macquarie Street
Sydney NSW 2000

By email: PortfolioCommittee1@parliament.nsw.gov.au

Inquiry into Cybersecurity

Dear Ms Moriarty,

Thank you for your invitation of 20 August 2020 to make a submission to the Committee's Inquiry into Cybersecurity (the Inquiry).

The Office of the Australian Information Commissioner (OAIC) is an independent Commonwealth regulator, established to bring together three functions: privacy functions (protecting the privacy of individuals under the *Privacy Act 1988* (Cth) (Privacy Act), freedom of information functions (access to information held by the Commonwealth Government in accordance with the *Freedom of Information Act 1982* (Cth)), and information management functions (as set out in the *Information Commissioner Act 2010* (Cth)).

I note that the Inquiry will consider, amongst other matters, cybersecurity and digital information management, including the monitoring and response to cybersecurity incidents and data breaches across the NSW Government.

Under the Privacy Act, the OAIC has oversight of the mandatory Notifiable Data Breaches (NDB) scheme, which commenced in February 2018. The NDB scheme has provided the OAIC with valuable insights into the reasons data breaches have occurred, and how entities can improve their security posture and processes to minimise the risks of a data breach. While the NDB scheme does not apply to NSW Government agencies, I draw on this regulatory experience in this submission to assist the Committee in its consideration of issues related to the monitoring and response to cybersecurity incidents and data breaches across the NSW Government.

Reporting statistics from the NDB scheme have consistently shown that malicious or criminal attacks are the main source of data breaches, reflecting the continued

challenge organisations and governments face in mitigating cybersecurity threats.[1] In these circumstances, mandatory notification can be an important mitigation strategy that can benefit both the entity and the individuals affected by a data breach. The OAIC also sees the intersection of data breaches affecting both State agencies and entities covered by the Privacy Act in the course of its regulatory work, and the resultant fragmentation of responsibilities and rights regarding data breaches that transcend jurisdictional borders.

One of the objects of the Privacy Act is to provide the basis for nationally consistent regulation of privacy and the handling of personal information. Accordingly, the Committee may wish to consider recommending a mandatory data breach notification scheme in NSW that aligns with the requirements of the NDB scheme under the Privacy Act. For the reasons set out below, we suggest national consistency of privacy regulation should be a key goal in the design of any state or territory-based mandatory data breach notification scheme and the Privacy Act provides the basis for achieving this consistency. Alignment with the requirements of the NDB scheme would ensure that Australians' personal information is subject to similar protections across jurisdictions, reduce compliance burdens and cost, ensure consumers receive consistent information about data breaches that may affect them, and provide clarity and simplicity for regulated entities and the community.

Purpose and operation of the NDB scheme

The NDB scheme requires Commonwealth Government agencies and private sector organisations covered by the Privacy Act to notify affected individuals and the OAIC of certain data breaches. The NDB scheme replaced the voluntary data breach notification scheme that had been in operation at the Commonwealth level since 2008.

The primary purpose of the NDB scheme is to ensure individuals are notified if their personal information is involved in a data breach that is likely to result in serious harm ('eligible data breach').[2] This has a practical function: once notified about a data breach, individuals can take steps to reduce their risk of harm. For example, an individual can change passwords to compromised online accounts, and be alert to identity fraud or scams.[3] Entities also have an obligation under the NDB scheme to

---

[1] The OAIC regularly publishes NDB statistics to help organisations, agencies and the public understand the operation of the NDB scheme. These reports are available on the OAIC's website at https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/.

[2] s 26WE *Privacy Act 1988* (Cth).

[3] Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016.

assist individuals by providing recommendations on what steps they can take to reduce harm they may experience as a result of the data breach.

An eligible data breach occurs when the following criteria are met:

- there is unauthorised access to, or disclosure of, personal information held by an entity (or information is lost in circumstances where unauthorised access or disclosure is likely to occur)
- this is likely to result in serious harm to any of the individuals to whom the information relates[4]
- the entity has been unable to prevent the likely risk of serious harm with remedial action.[5]

If an entity suspects that an eligible data breach has occurred, they must undertake a reasonable and expeditious assessment into the relevant circumstances.[6] An entity must take all reasonable steps to complete the assessment within 30 calendar days. I generally expect entities to treat 30 days as the maximum time limit for completing an assessment, and they should endeavour to complete the assessment in a much shorter timeframe. In the event of an eligible data breach, an entity is required to notify the Commissioner and affected individuals as soon as practicable after the entity is aware that there are reasonable grounds to believe that there has been an eligible data breach (unless an exception applies).[7]

Careful consideration needs to be given to statutory timeframes for the assessment and notification of data breaches to balance the ability of entities to complete an investigation to assess the level of risk associated with a suspected breach, with the timely notification to individuals so they may take steps to mitigate the risk of harm. The statutory timeframes set out in the NDB scheme are intended to provide flexibility for entities to scale their response to the particular facts and circumstances of a data breach. That is, the amount of time and effort entities will expend in an assessment should be proportionate to the likelihood of the breach and its apparent severity. However, I generally expect entities to complete their assessment of a suspected eligible data breach, and notify individuals (if the entity believes that there

---

[4] s 26WE(2) *Privacy Act 1988* (Cth).

[5] s 26WF *Privacy Act 1988* (Cth).

[6] s 26WH *Privacy Act 1988* (Cth).

[7] s 26WK *Privacy Act 1988* (Cth).

has been an eligible data breach), expeditiously as the risk of serious harm to individuals often increases with time.[8]

It is important to note that the NDB scheme is designed so that only data breaches that meet the 'serious harm' threshold are notifiable. Sometimes, notifying individuals where there is very little or no risk of harm can cause unnecessary anxiety. It can also de-sensitise individuals so that they do not take a notification seriously, even where there is a real risk of serious harm. Serious harm, in this context, could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm that a reasonable person in the entity's position would identify as a possible outcome of the data breach.[9]

The NDB scheme also serves the broader purpose of enhancing entities' accountability for privacy protection. By demonstrating that entities are accountable for privacy, and that breaches of privacy are taken seriously, the NDB scheme works to build trust in personal information handling and data sharing across the private and public sectors.

Failure to comply with an obligation under the NDB scheme will be deemed to be an interference with the privacy of an individual for the purposes of the Privacy Act. This will engage my existing powers to investigate, make determinations and provide remedies in relation to non-compliance with the Privacy Act. This includes the capacity to undertake Commissioner initiated investigations, make determinations, seek enforceable undertakings, and pursue civil penalties for serious and repeated interferences with privacy.

The OAIC's role in the NDB scheme and key learnings

Under the NDB scheme, the OAIC:

- receives notifications of eligible data breaches

---

[8] See the OAIC's *Data breach preparation and response* guide available at https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/.

[9] Section 26WG of the *Privacy Act 1988* (Cth) sets out relevant matters that an entity should consider in determining whether a reasonable person would conclude that a data breach would be likely, or would not be likely, to result in serious harm. More information about what constitutes 'serious harm' can also be found in the Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016 and the OAIC's *Data breach preparation and response* guide available at https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/.

- encourages compliance with the NDB scheme, including by handling complaints, conducting investigations and taking other regulatory action
- offer advice and guidance to regulated organisations[10]
- provides information to the community about the operation of the NDB scheme.

The NDB scheme has provided the OAIC with visibility into how Australian entities are meeting the challenges associated with protecting personal information. The introduction of the NDB scheme in February 2018 resulted in a 712 per cent increase in total data breach notifications over the first 12-months of its operation compared with the previous 12 months under the voluntary scheme.[11]

The NDB scheme also shed light on the causes of data breaches, allowing the OAIC and entities to better understand how they might be avoided and implement prevention strategies. As outlined above, malicious or criminal attacks were the main source of data breaches in the NDB scheme's first year (and continue to be in the period since).[12] However, most data breaches, including those resulting from a cyber incident, involved a human element, such as an employee sending information to the wrong person or clicking on a link that resulted in the compromise of user credentials.

As outlined above, the key objective of the NDB scheme is to enable individuals to take steps to mitigate the risk of harm that may arise from a data breach. The first year of the NDB scheme in operation provided numerous examples of organisations taking immediate steps to reduce further harm to affected individuals. A best practice example involved a reporting entity using social workers to notify affected individuals by phone in the context of a data breach impacting a vulnerable segment of the community. In addition to providing information about the data breach and recommended steps to reduce harm, the social workers also asked questions to identify any individuals at higher risk of harm and accordingly made appropriate referrals for further support.[13]

---

[10] See the OAIC's *Data breach preparation and response* guide available at https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/

[11] See the OAIC's *Notifiable Data Breaches scheme 12-month insights report*, May 2019, available at https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/

[12] The OAIC's Notifiable data breaches statistics are available at https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/.

[13] See the OAIC's *Notifiable Data Breaches scheme 12-month insights report*, May 2019, available at https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/

The OAIC publishes NDB statistics every six months to help organisations, agencies and the public understand the operation of the NDB scheme and the causes of data breaches. Our Insights Report, released in May 2019, outlines the lessons learned during the first year of the NDB scheme and gives best practice recommendations. The statistics and insights reports are available on the OAIC's website at https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/.

Benefits of a state-based mandatory notification scheme

The OAIC notes that NSW currently has a voluntary data breach notification scheme. The voluntary scheme encourages agencies that have experienced a serious data breach to report the details of the breach to the NSW Privacy Commissioner, so the Commissioner can assess the breach, provide advice or investigate.[14]

A voluntary scheme means that some entities may not notify individuals in the event of a serious data breach which can increase the risk of harm to those individuals. Conversely, notification is not always an appropriate response to a breach. As outlined above, notifying individuals where there is a minimal risk of harm can cause unnecessary anxiety and lead to 'notification fatigue', which can result in individuals failing to take a data breach notification seriously even where there is a real risk of serious harm. Consequently, a key challenge for government agencies is to determine when to notify individuals and the regulator. A mandatory notification scheme carries a number of benefits including:

- providing clarity for entities as to the kinds of data breaches that need to be notified and expected timeframes for notification, and
- providing consumers with confidence that they will be advised if their personal information is compromised and more comprehensive and consistent information about data breaches that may affect them and how they might mitigate associated risks.

A mandatory scheme can also increase understanding of causes and sectoral trends, and can drive real improvements to people, process and technology measures which prevent data breaches. For instance, since the NDB scheme commenced, the OAIC has observed efforts by many entities to lift their practices, such as by developing and implementing data breach response plans and improving security and privacy

[14] Information and Privacy Commission NSW, *Data Breach Guidance for NSW Agencies* available at https://www.ipc.nsw.gov.au/data-breach-guidance-nsw-agencies

standards, and efforts by some entities in adopting data minimisation policies to reduce overall exposure.[15]

More broadly, Commonwealth, State and Territory governments are increasingly working together on national initiatives that involve sharing information across jurisdictions. In many instances, these initiatives rely on jurisdictions across Australia having privacy frameworks that are equivalent to the protections afforded by the Commonwealth Privacy Act, including commensurate protections for personal information such as mandatory data breach notification requirements.

One of the objects of the Privacy Act is to provide the basis for nationally consistent regulation of privacy and the handling of personal information.[16] A state-based scheme that aligns with the requirements of the NDB scheme under the Privacy Act would ensure that Australians' personal information is subject to similar protections whether that personal information is being handled by an Australian Government agency or a state or territory government agency, or private sector organisations.

Consistency in regulation across jurisdictions will also reduce compliance burdens and cost, and provide clarity and simplicity for regulated entities and the community. National consistency, therefore, is a key goal of mandatory data breach notification schemes and privacy regulation more broadly.

Should you require further information about the operation of the NDB scheme or any aspect of this submission please contact Sarah Croxall, Director, Regulation and Strategy Branch

Yours sincerely

Angelene Falk
Australian Information Commissioner
Privacy Commissioner

21 September 2020

---

[15] See the OAIC's *Notifiable Data Breaches scheme 12-month insights report*, May 2019, available at https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/

[16] s 2A, *Privacy Act 1988* (Cth)