MERIDIAN LAWYERS

October 2017

Health insights

Massive privacy breach: A lesson in using third party web service providers

By Marianne Nicolle, Principal
T 02 4047 2611
E mnicolle@meridianlawyers.com.au

By Anna Martin, Associate
E amartin@meridianlawyers.com.au

The potential for inadvertent privacy breaches in the age of third party web providers became all too apparent for the Australian Red Cross Blood Service (the "Blood Service") recently, after it was discovered that the personal information relating to approximately 550,000 prospective blood donors was leaked on 5 September 2016.

The circumstances of the breach concerned information that had been entered by prospective blood donors into a public-facing website called "Donate Blood.com.au". The website was managed by a third party provider who hosted the non-production environment for the site, including a copy of the live website and a copy of customer data entered by individuals on the site.

The information collected from individuals included personal details such as age, gender, address and whether the person had engaged in high-risk sexual activity. This data was used by the Blood Service to make appointments for prospective donors. Once collected by the website, the information was then entered by Blood Service employees into the internal Blood Service management system. However, a copy of the information was also retained on the "backend" of the website, which was maintained by the third party provider in a secure location.

On 5 September 2016, an employee of the third party provider accidentally created a backup of the "backend" database file and saved it to a publically accessible area (instead of the intended secure destination). The breach was detected by an individual who alerted it to cyber security organisations.

Once notified, the Blood Service took full responsibility for the breach. It co-operated with the Australian Cyber Emergency Response Team to assist its response to the incident and engaged a separate entity to complete an independent risk assessment of the personal information compromised. The Blood Service also took steps to notify the public and affected individuals. By way of forensic analysis, it was able to confirm that there had only been four requests to download the data file, and that all copies had been deleted.[1]

Interestingly, despite the circumstances described above, the Office of the Australian Information Commissioner (the "Commissioner") concluded that the Blood Service had not breached Australian Privacy Principle 6 (APP 6), which "regulates the use and disclosure of personal information and states that organisations may only use or disclose personal information for the primary purpose of collection, unless an

exception applies".[2] This was because the breach in this case was caused by a human error on the part of the third party provider, without the authorisation or direct involvement of the Blood Service. It was also outside the scope of the third party's contractual obligations to the Blood Service. The Commissioner did not hold the Blood Service responsible for the disclosure itself.

However, the Blood Service was held responsible for breaching both APP 11.1 and 11.2 which are respectively summed up by the Commissioner in its Investigation Report as relating to:

- requiring organisations to take such steps as are reasonable in the circumstances to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure. This applies where the information is in the organisation's physical possession, or where it has the right or power to deal with the information even if it does not physically possess it or own the medium on which the information is stored (in respect of APP 11.1);[3] and
- requiring organisations to take reasonable steps to destroy or de-identify information it no longer needs for any purpose for which the information may be used or disclosed under the APPs (in respect of APP 11.2).[4]

The Commissioner considered that the contractual relationship between the Blood Service and the third party provider was such that the Blood Service retained effective ownership of the data concerned, and therefore both organisations had an obligation under APP 11.1 to protect it. Furthermore, the sensitivity of the data increased the degree to which it needed to protected.

The Commissioner also acknowledged that although the Blood Service had a security framework in place including documented information security policies and regular staff training, the Blood Service had not assessed the adequacy of the third party provider's own security measures and practises when it entered into the contract for services. Among other things,

The Blood Services' requirements of (the third party provider) in relation to information security were not clearly articulated or proportional to the scale and sensitivity of the information held by the Blood Service and the third party provider.

A reasonable step in the circumstances may have been to include specific contractual requirements for how (the third party provider) would handle and store the personal information of blood donors on the Donate Blood website, and a reporting mechanism for the Blood Service to ensure these contractual requirements were being met.[5]

With respect to the breach of APP 11.2, the Commissioner found that once the information entered into the Donate Blood.com.au website had been recorded in the Blood Service's internal management system, the personal information was no longer needed for the purpose for which it was collected (or any other function or activity of the Blood Service). As such, it should have been destroyed or de-identified after a defined period. The failure to do so was a contributing factor to the breach.

It is worth mentioning here, that despite the above findings the Commissioner commended the Blood Service's response to the privacy breach. The quick and effective action taken by the organisation once notified of the breach held it in good stead with the Commissioner in the course of its investigation, the result of which was to accept an enforceable undertaking from the Blood Service "formalising its commitment to review certain measures with a specific timeframe".[6] For completeness, we note that the steps required of entities responding to privacy breaches will soon be impacted by new amendments to the *Privacy Act 1988* (Cth), which come in to effect on 22 February 2018 .[7] The changes will oblige entities currently bound by the APPs to comply with mandatory notification requirements in certain circumstances.

The full details of this case are recounted in the Commissioner's Investigation Report which is published here (https://www.oaic.gov.au/resources/privacy-law/commissioner-initiated-investigation-reports/donateblood-com-au-data-breach-australian-red-cross-blood-service.pdf). It provides insights into the level of data security measures previously maintained by the Blood Service, and the additional steps which were necessary following the breach. It serves as a useful case study for organisations which may be using, or wish to use, third party providers to maintain web services including sensitive database files.

Meridian Lawyers can assist you to understand your privacy obligations, particularly in light of impacts made by the *Privacy Amendment (Notifiable Data Breaches) Act 2017*.

THIS ARTICLE WAS WRITTEN BY PRINCIPAL MARIANNE NICOLLE AND ASSOCIATE ANNA MARTIN. PLEASE CONTACT US IF YOU HAVE ANY QUESTIONS OR FOR FURTHER INFORMATION.

[1] DonateBlood.com.au data breach (Australian Red Cross Blood Service), Investigation Report of the Office of the Australian Information Commissioner, dated 7 August 2017, pages 5 & 6.

[2] Ibid, page 8.

[3] Ibid, page 9.

[4] Ibid, page 12.

[5] Ibid, page 11.

[6] Ibid, page 15.

[7] As per the *Privacy Amendment (Notifiable Data Breaches) Act 2017*.