Australian Government

Office of the Australian Information Commissioner

7 August 2017

DonateBlood.com.au data breach (Precedent Communications Pty Ltd)

Investigation Report

www.oaic.gov.au

Contents

Executive Summary

Precedent Communications Pty Ltd (**Precedent**) managed the website www.donateblood.com.au for the Australian Red Cross Blood Service (**the Blood Service**).

On 5 September 2016, a Precedent employee inadvertently saved a backup of a database file containing information relating to approximately 550,000 prospective blood donors, who had entered their details on the Donate Blood website, to a public-facing web server (**the data breach**). The data file was discovered and accessed by an unknown individual on 25 October 2016. On the same day, the individual notified the Blood Service via a number of intermediaries. The Blood Service immediately took steps to contain the breach.

On 27 October 2016, the Australian Information Commissioner (the **Commissioner**) opened an investigation into the incident under s 40(2) of the *Privacy Act 1988* (Cth) (**Privacy Act**). The Commissioner's decision to investigate this incident was made in light of the large number of Australians whose personal information was involved, and the sensitivity of the data. The Commissioner's investigation considered whether Precedent's information handling practices met the requirements of the Privacy Act. The Commissioner also opened a separate investigation into the Blood Service.

The root cause of the data breach was an unforeseen one-off human error on the part of a Precedent employee. However, the error was made in the course of that individual's duties, and as such the data breach was a 'disclosure' within the meaning of Australian Privacy Principle (**APP**) 6.

Precedent breached the Privacy Act in respect of APP 6 and APP 11 by:

- disclosing the personal information of individuals who had made an appointment on the Donate Blood website, in breach of APP 6
- failing to take reasonable steps to adequately mitigate against the risk of a data breach, and to protect the personal information it held from unauthorised disclosure, in contravention of APP 11.1.

The findings of this report include important lessons for other organisations, illustrating how a number of security deficiencies can create a situation in which human error can trigger a data breach. Organisations should have sufficient protections in place to ensure that even if there is a failure at one point, the protections inherent in the other levels will prevent the breach from occurring.

Although Precedent had not met all the requirements of the Privacy Act, the Commissioner acknowledges Precedent's constructive and cooperative approach in working with the OAIC in this matter. The Commissioner also acknowledges that in response to this incident, Precedent has invested significant effort to improve its information handling practices, strengthen its information security, and ensure that it is now compliant with the Privacy Act.

To assure the Commissioner and the Australian community that Precedent will address the issues identified in the investigation, Precedent offered, and the Commissioner accepted, an enforceable undertaking on 28 July 2017.

Background

Precedent and the Donate Blood website

Precedent is a digital agency that provides services, including technical development and support, for clients' websites. In 2014, Precedent was awarded the contract to re-develop the Blood Service's desktop and mobile Donate Blood websites into one platform with additional capabilities. After the new Donate Blood website was launched in 2015, Precedent was also awarded the contract for the Donate Blood website development and application support, ongoing management, consulting and testing, and maintenance and upgrades.

At the time of the incident, information entered by potential donors remained on the 'backend' of the Donate Blood website, as well as being transmitted to the Blood Service. The production environment of the website (the live, user-facing version of the website) was hosted for Precedent by Amazon Web Services. Non-production environments, including the website's User Acceptance Testing (**UAT**) environment were hosted and managed by Precedent directly. The UAT environment held a copy of the website, including customer data which was 'refreshed' on a monthly basis.

Precedent describes the purpose of the UAT environment as follows:

> Precedent developers used this server for deploying new code & functionality for donateblood.com.au in order to test it prior to being pushed to Production (Live) in AWS Amazon Web Services (AWS). The client (ARCBS) was using two sites on the affected environment, with one site being dedicated to business-as-usual (BAU) support & the secondary site being used for a project to implement a new CRM.
>
> The two test sites were used for a range of reasons such as:
>
> - testing new functionality
> - testing new content creation
> - occasionally being utilised as a guided training platform for staff across ARCBS including from their National Contact Centre[1].

The data breach

The UAT environment contained a copy of all data entered into the production version of the Donate Blood website. The actual UAT environment was protected by Precedent through a number of mechanisms (including password access). However, portions of the web server on which the UAT environment was located were publicly accessible.

On 5 September 2016, a Precedent employee tasked with enhancing a feature on the Donate Blood website created a database backup of the UAT database file (the **data file**) on the UAT environment before making changes to the system. The backup would have allowed for the restoration of data should an error occur during development work or database upgrades. The employee had intended to save the data file created to a secure location but, in error, saved the data file to a publicly accessible portion of the web server on which the UAT environment was implemented.

[1] Precedent's submission to the OAIC, 5 December 2016, p 3.

The data file contained registration information of the 550,000 prospective donors who requested an appointment to donate blood via the website between 2010 and 5 September 2016.

The data file included the personal information of approximately 550,000 individuals who had expressed an interest in donating blood on the Donate Blood website. The file also included sensitive information about some of the individuals. The file contained all information collected via the website, and included contact information and health information used to assess each individual's eligibility to donate blood.

The categories of personal information collected via the Donate Blood website included:

- identifying particulars: first and last name, gender, date of birth and donor ID (optional)
- contact details: physical address, email address and phone number
- appointment preferences: postcode or suburb for donation, preferred date range request for donation and preferred time of day
- yes or no responses to donor eligibility questions: for example whether or not the prospective donor is taking antibiotics, had engaged in risky sexual behaviour or if they are or have been pregnant in the last nine months.

Post-incident response

On 25 October 2016, the data file was accessed and copied by an individual scanning for security vulnerabilities. This individual then contacted Troy Hunt, a cybersecurity expert who operates the blog www.troyhunt.com and data breach notification service www.haveibeenpwned.com. Mr Hunt subsequently informed the Australian Cyber Emergency Response Team (**AusCERT**).

AusCERT coordinated a response to the incident and notified the Blood Service.

In response to a request from AusCERT, the Internet Service Provider (**ISP**) responsible for hosting the UAT environment removed access to the UAT environment at approximately 22:45 on 25 October 2016. As a result the file was no longer accessible. The ISP notified Precedent of the data breach on 26 October 2016.

After becoming aware of the compromise of the data, Precedent responded in a support capacity by cooperating with the Blood Service in their investigation. Precedent provided the compromised server to the Blood Service for an external forensic investigation, and at the direction of the Blood Service, deleted all data stored on the Donate Blood website.

Commissioner's investigation

Under s 40(2) of the Privacy Act, the Commissioner may, on the Commissioner's own initiative, investigate an act or practice that may be an interference with privacy.

On 27 October 2016, the Commissioner commenced an investigation into this incident, with a focus on whether Precedent took reasonable steps to protect the personal information that it held from misuse and loss and from unauthorised access, modification and disclosure. The investigation also considered the steps taken by Precedent following the incident to mitigate the impact of the data breach and minimise the chance of reoccurrence.

Relevant provisions of the Privacy Act

The Privacy Act applies to all private sector organisations with an annual turnover of more than $3 million and some small businesses. Organisations covered by the Privacy Act must comply with the APPs contained in Schedule 1 of the Privacy Act. The APPs apply to the handling of 'personal information', which section 6 of the Privacy Act defines as:

> information or an opinion about an identified individual, or an individual who is reasonably identifiable:
>
> (a) whether the information or opinion is true or not; and
>
> (b) whether the information or opinion is recorded in a material form or not.

APP 6 states that an organisation must only use or disclose personal information for the primary purpose of its collection, unless it can rely on exceptions described under APP 6.1(a) – (b).

APP 11 states that an organisation must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

Disclosure of personal information (APP 6)

APP 6 regulates the disclosure of personal information and states that an entity may only use or disclose an individual's personal information for the primary purpose of collection, unless an exception applies.

The Office of the Australian Information Commissioner (**OAIC**) has published the *Australian Privacy Principle Guidelines* (**APP Guidelines**), which state that an organisation 'discloses' personal information when it makes the information accessible to others outside the organisation and releases the subsequent handling of the personal information from its effective control. The release may include an accidental release or an unauthorised release by an employee.[2]

Under s 8(1)(a) of the Privacy Act, an act or practice engaged in by a person employed by, or in the service of an organisation in the performance of the duties of the person's employment shall be treated as having been engaged in by the organisation. In this incident, a Precedent employee erroneously placed the data file in a location that was publicly accessible, and where a member of the public was subsequently able to download a copy of the data file. As this was done by a person employed by Precedent, in the performance of the duties of the person's employment, it is therefore considered an act undertaken by Precedent.

Given that an act by Precedent made the personal information accessible to others outside of the organisation, and as the data file was no longer in Precedent's effective control once it was downloaded by the third party, Precedent 'disclosed' the data file within the meaning of APP 6.

Whether disclosure permitted by APP 6

Precedent's stated purpose for the collecting personal information via a monthly 'refresh' of the live production, was for Precedent to 'test any new functionality with real data'.[3] The disclosure of personal information on a publicly accessible portion of Precedent's web server was not for the primary purpose for which it was collected.

APP 6.1 states that an organisation must not disclose personal information for a purpose other than the primary purpose unless a relevant exception under APP 6.1(a) or APP 6.1(b) applies. There is no information to suggest that any of the exceptions applied to the data breach incident. Therefore, Precedent's disclosure of personal information was not permitted by APP 6.1.

Findings

Precedent disclosed the personal information contained in the data file in breach of APP 6.1.

[2] Paragraphs [B.64] and [6.10], available online at https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/.

[3] Precedent's submission to the OAIC, 5 December 2016, p 3.

Protection of personal information (APP 11.1)

APP 11.1 requires organisation to take reasonable steps in the circumstances to protect personal information held by the entity from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

APP 11.1 applies to personal information 'held' by an organisation. Information is held by an organisation where it has physical possession of the data or the right or power to deal with the information.

Whether a breach of APP 11.1 has occurred depends on if, at the time of the incident, an organisation had taken reasonable steps in the circumstances to protect the personal information it held. Where there is a known risk to data security, APP 11 would generally require that an APP entity take reasonable steps to mitigate that risk.

Practices at the time of the data breach

The *Service Agreement* between the Blood Service and Precedent signed 18 September 2014 included the requirement that:

> The Supplier will comply with, and will ensure that its Personnel comply with, any policies or procedures notified by the Blood Service to the Supplier from time to time, including without limitation any policies relating to privacy, security, computer resources, Occupational Health & Safety and code of Good Manufacturing Practice (GMP) Awareness Training, where applicable.

A *Confidentiality Agreement* between the Blood Service and Precedent signed 18 September 2014 included the requirement that:

> The Recipient must protect all Confidential Information from unauthorised access or use, and must take and enforce proper and adequate precautions at all times to preserve the secrecy and the confidentiality of all Confidential Information.
>
> If the Recipient… breaches or is likely to breach any obligation or confidentiality arising under this Agreement, the Recipient must take reasonable steps to limit the consequences of that breach and to prevent any further breach.

This agreement indicates that Precedent had committed to protect the information it held on behalf of the Blood Service.

Precedent provided the OAIC with details of its technological and organisational safeguards in place at the time of the data breach. These included:

- **Technological safeguards:** IP authentication is used for all client environments including test environments. Database servers are not addressed publicly and are only available on a web server via Secure Sockets Layer (SSL). SSL encryption is in place on web traffic, form submissions and log-ins. Precedent recommends the use of obfuscated data in all areas where possible

- **Risk assessment:** a 'risk register' is created at the start of every client project, and regularly reviewed and updated. Precedent's *Risk Management Policy* outlines organisational objectives and risk identification, response and monitoring procedures and responsibilities, and

- **Organisational safeguards:** Precedent's data protection policy was the *Data Protection Act 2016 – 2017*. The policy includes a *Confidentiality Statement for Staff*, outlining Precedent's expectation that employees only access or use information they are authorised to. Staff are instructed to not compromise or seek to evade security measures and to be careful when handling confidential information.

  Staff training on their data security obligations consisted of the requirement to read the Data Protection Act and watch a video produced by the UK Information Commissioner's Office on data protection during the standard induction process. In July 2013, a request was sent to all staff to read the updated Data Protection Policy and watch the same video.

With regard to Precedent's management of the Donate Blood website:

- IP authentication was not implemented. Precedent indicated that this was because the Blood Service used a content filtering and security cloud service that was not compatible with Precedent's IP authentication system. As such, an internet user was able to access the relevant server if they knew its location. Precedent allege that a contributing factor to this privacy incident was the Blood Service not meeting Precedent's request for a proxy bypass to allow the use of IP Authentication. While this is disputed by the Blood Service, it is not necessary to resolve this disagreement as the lack of IP authentication was only one point in a chain of issues that lead to the breach.

- A 'risk register' was not completed for the project. Precedent stated that it did not treat support agreements (such as the one held with the Blood Service) as a project. The risk of a data breach was not identified in the Donate Blood website re-development project or the Blood Service Development & Application support contract.

- Precedent's *Risk Management Policy* did not address information security relating to the handling of personal information, or document procedural requirements for Precedent employees with regard to its privacy obligations.

- One of the employees involved in the incident had not read the *Data Protection Policy* at the commencement of employment; due to human error and miscommunication, this was not followed up on. The two Precedent employees involved in this incident had not received any additional privacy training at Precedent.

- Precedent did not undertake steps to satisfy itself of the adequacy of its existing security measures and states that it has 'not recently sought any relevant expert advice on this topic, nor conducted a relevant risk assessment at organisational level'.[4]

Steps to reduce risk of human error

In order for policies and procedures to constitute a reasonable security safeguard, those policies and processes must adequately address known risks.[5] The OAIC's *Guide to securing personal information* (**the PI Security Guide**) specifies that entities should assume that human error will occur and design their policies and procedures to mitigate this risk, as organisational failures may combine to create a situation in which a human error can result in a data breach.[6]

[4] Precedent's submission to the OAIC, 5 December 2016, p 11.

[5] See Department of Immigration and Border Protection: Own motion investigation report AICmrCN 5.

[6] OAIC Guide to securing personal information, January 2015, page 10. Available online at https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information.

The UAT environment used live data from the Donate Blood website, although this did not appear to be a necessary business requirement at the time of the incident and Precedent indicated that its general practice was to use obfuscated data. The PI Security Guide outlines that when personal information is used for testing Information Communication and Technology (**ICT**) systems, a reasonable step to ensure this information remains secure would be to conduct a privacy impact assessment and information security risk assessment to assess the personal information flows caused by the testing.[7]

While the employee in this instance did not follow correct processes in relation to where a data backup should be stored, Precedent has also advised that 'the developer who ran the back-up command may not have been aware that the location the data was placed in was insecure'.[8] Precedent does not appear to have had internal practices or procedures in place to mitigate against any risks associated with using live data in these circumstances, such as ensuring its employees were aware of which data locations were secure. Given that Precedent made regular back-ups of the database containing the live data, one such procedure may also have included keeping a backup log.

Security policies and procedures should not only cover preventive measures, but also pro-active measures to limit the adverse impact of human error. The PI Security Guide provides that if an organisation stores content on a server that is not intended to be disclosed to the public, it is reasonable to regularly review and monitor the server to ensure the content is not being accessed by unauthorised persons. Additionally, the PI Security Guide recommends that organisations disable directory browsing to prevent an unauthorised person from viewing a list of the files on the server.

In this instance there is no apparent business reason for Precedent to locate the UAT environment on a server that was partially accessible to the public. At the time of the incident, Precedent had not disabled directory browsing on the affected server. With regard to Precedent's business activities, these systems may have included a periodic audit of the files on the server to identify anomalous files, or the use of access monitoring software to provide a real time review of access activity by external users. These measures may have alerted Precedent to the vulnerability earlier or mitigated the consequences of the error. As a result of the failure to plan for these risks, Precedent was not aware that the data file was in an insecure location and publicly accessible for about 50 days.

Findings

While it appears that Precedent considered its obligations under the Privacy Act, and took steps to implement a security framework, it did not have adequate measures in place to ensure the relevant policies and procedures were consistently applied. Consequently, it does not appear that Precedent took reasonable steps to identify potential risks and implement specific systems to protect the personal information it held from unauthorised disclosure, as required by APP 11.1.

The Commissioner is of the view that the steps that Precedent took to protect the personal information it held were lacking in the following key elements:

- A focus on risk management as it relates to personal information – Precedent did not consistently apply its *Risk Management Policy*, and failed to ensure that its information security arrangements were, and remained, commensurate to the type and sensitivity of the personal information it was handling.

[7] OAIC *Guide to securing personal information*, January 2015, p 26.

[8] Precedent's submission to the OAIC, 5 December 2016, p 6.

- Live data was used for testing purposes on the UAT environment, when dummy data would have sufficed.

- Monitoring systems and quality assurance processes – given that Precedent was using live data, it did not have any processes in place to track any database back-ups, or take steps to control for the possibility of human error by reducing and restricting access to its systems.

On this basis, the Commissioner's view is that Precedent failed to adequately mitigate against the foreseeable risk of human error resulting in a data breach. Precedent did not take reasonable steps to protect the personal information held on the Donate Blood system from misuse and loss and from unauthorised access, modification or disclosure, in contravention of APP 11.1.

Rectification

The Commissioner considered the information that Precedent provided about the steps that it took to respond to and contain the data breach, and to mitigate against future data breaches of this nature. Overall, Precedent acted appropriately in response to the incident by working closely with the Blood Service to investigate and rectify the incident.

Since the data breach, Precedent has undertaken technical, procedural and organisational remediation steps to enhance its privacy and data security safeguards and prevent future breaches of this nature. Particular measures Precedent has taken include:

- assessing all Precedent client environments including UAT (test) and production (live) environments to ensure they are appropriately secure and introduced enhanced vulnerability testing
- engaging an independent organisation to review its technical development processes and management of technical environments, with a focus on data security
- engaging external consultants to conduct an independent data security review of its systems and practices, which commenced on 28 November 2016
- updating Precedent project templates such as the Risk Register and Project Initiation Document with mandatory items regarding data protection, such as:
    - a risk register containing a standard, pre-filled risk of data breach, which must be mitigated against for all projects
    - a Project Initiation Document containing specific data protection items, such as whether Precedent is required to store or transfer personal data as part of this project, including a specific check of what data does and does not need to be stored and/or transferred by Precedent for the purposes of the project.
- instituting regular data privacy training for all employees, and made the enhanced training part of the new employee induction process.

Conclusion

The Commissioner found that Precedent breached the Privacy Act in respect of APP 6 and APP 11.1 by:

- disclosing the personal information of individuals who had made an appointment on the Donate Blood website, in breach of APP 6
- failing to take reasonable steps to adequately mitigate against the risk of a data breach, and to protect the personal information it held from unauthorised disclosure, in contravention of APP 11.1.

Precedent acted appropriately in response to the data breach and the Commissioner acknowledges the extensive remedial action Precedent has taken since the incident. The Commissioner also acknowledges Precedent's cooperation, timely responses and openness to consider recommendations throughout this investigation.

In considering what further regulatory action to take, the Commissioner invited Precedent to provide a substantive response outlining the steps it intends to take to improve the inadequacies identified by the investigation in relation to Precedent's relevant policies and procedures.

In response, Precedent proposed an appropriate set of measures to enhance its protection of personal information and the Commissioner accepted an enforceable undertaking from Precedent formalising its commitment to implement these measures within a specified timeframe. Based on Precedent's ongoing implementation of the measures proposed to enhance its protection of personal information, the Commissioner considers this an appropriate conclusion to the investigation.