

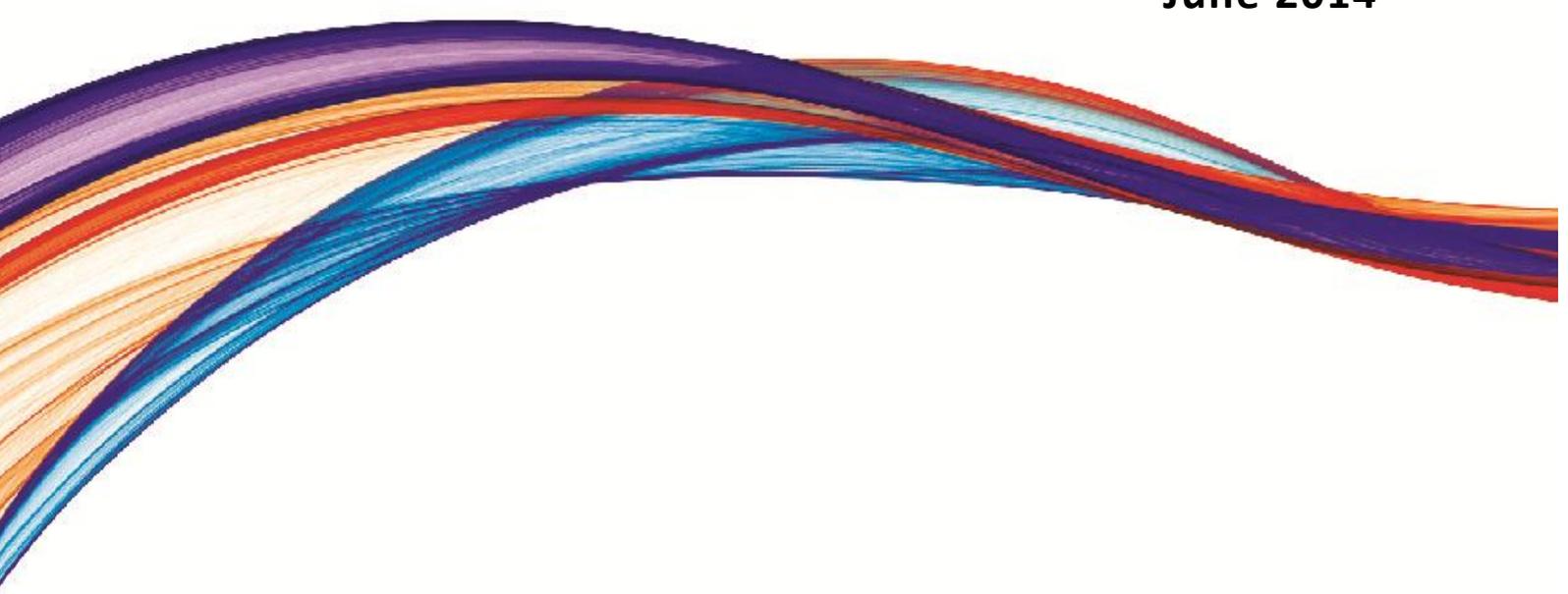


Australian Government

Office of the Australian Information Commissioner

Cupid Media Pty Ltd Own motion investigation report

June 2014



Timothy Pilgrim, Australian Privacy Commissioner

Contents

Overview.....	3
Background.....	3
Relevant provisions of the Privacy Act	4
Findings.....	5
Security of personal information (NPP 4.1).....	5
Nature of personal information.....	5
Information and patch management	6
Testing and monitoring.....	6
Passwords and encryption.....	7
Secure destruction or permanent de-identification of personal information that is no longer required (NPP 4.2)	8
Disclosure of personal information (NPP 2.1)	8
Rectification.....	9
Recommendations.....	10
Conclusion	10
Acronyms and abbreviations	11

Overview

Cupid Media Pty Ltd (Cupid) operates over 35 niche dating websites based on personal profile including ethnicity, religion and location. On 13 December 2013, the Australian Privacy Commissioner (the Commissioner) opened an own motion investigation into Cupid. This was in response to media allegations that personal information of Cupid users had been acquired by unauthorised persons, and were found on a server operated by hackers, which Cupid confirmed.

The Commissioner's investigation focused on whether Cupid took reasonable steps to protect user information from misuse, loss, unauthorised access, modification or disclosure.¹

After considering the facts of the case, submissions from Cupid and the relevant provisions of the *Privacy Act 1988* (Cth) (Privacy Act), the Commissioner came to the view that Cupid had breached the Privacy Act by failing to take reasonable steps to secure personal information it held.

The Commissioner however welcomed Cupid's collaborative and cooperative approach in working with the Office of the Australian Information Commissioner (OAIC) in this matter, and the significant privacy remedial steps that it took in response.

Background

On 21 November 2013, the OAIC received information that Cupid user records had been stolen and found on a server operated by hackers (data breach).

Cupid confirmed that the following key events led to the data breach:

- On 21 January 2013, Cupid identified a rogue file on one of its web servers.
- Cupid then conducted internal investigations and identified that on 18 January 2013, attackers exploited a vulnerability within the application server platform used by Cupid (ColdFusion), which allowed them to gain access to Cupid's web servers.
- With access to Cupid's web servers, the attackers were able to upload a shell 'ColdFusion Markup' (CFM) file that allowed the attackers to run SQL queries against Cupid's databases and gain unauthorised access to Cupid's data.²
- A security hotfix (patch) for the ColdFusion vulnerability was released on 16 January 2013, however Cupid did not receive notification from the developer that the patch was available. Cupid advised that the particular developer ordinarily sent Cupid an alert when updates and patches were made available, but did not do so in this instance. In the absence of the alert, Cupid's IT team

¹ As required under National Privacy Principle (NPP) 4.1.

² 'SQL' refers to a special purpose programming language (called Structured Query Language) designed for managing data held in a database management system.

identified (through its business as usual internal patch management processes) that the patch was available on 21 January 2013.

- On 21 January 2013, Cupid applied the patch and fixed the vulnerability, which in turn stopped the attackers from obtaining further data.

Cupid advised that the categories of personal information compromised in the data breach consisted of:

- (a) full names
- (b) dates of birth (for some customers)
- (c) email addresses, and
- (d) passwords.

Cupid explained that there is no requirement for Cupid's users to verify their name to open an account. For this reason, Cupid considers that some of the full names and associated dates of birth involved in the data breach 'did not relate to real persons'.

In any case, Cupid estimates that the accounts and personal information of approximately 254,000 Australian users were compromised in the data breach.

Relevant provisions of the Privacy Act

From 21 December 2001 to 11 March 2014, organisations covered by the Privacy Act were required to comply with the ten National Privacy Principles (NPPs), contained in Schedule 3 of the Act.³ The NPPs were replaced by the Australian Privacy Principles (APPs) on 12 March 2014.⁴

The NPPs applied to the handling of 'personal information' which the Privacy Act defined as:

information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Personal information includes 'sensitive information'. The Privacy Act's definition of 'sensitive information' prior to 12 March 2014⁵ included information or an opinion about an individual's:

- racial or ethnic origin;
- religious beliefs or affiliations; or

³ On 12 March 2014, the NPPs were replaced by the Australian Privacy Principles:

<http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles>.

⁴ See <http://www.oaic.gov.au/privacy/privacy-act/australian-privacy-principles>.

⁵ The definition of 'sensitive information' under the current Privacy Act is substantially similar to that which applied at the time of the data breach.

- sexual preferences or practices.

The Privacy Act applies to all private sector organisations with an annual turnover of more than \$3 million and some small businesses. A business with an annual turnover of less than \$3 million that trades in personal information was also covered by the NPPs.⁶ Cupid is subject to the Privacy Act and was subject to the NPPs at the time of the data breach.

NPP 4 (Data security) and NPP 2 (Use and disclosure) were the Privacy Act provisions relevant to this data breach. In particular:

- NPP 4.1 required organisations to take reasonable steps to protect the personal information they hold from misuse and loss and from unauthorised access, modification or disclosure⁷
- NPP 4.2 stated that, if an organisation no longer needs personal information for any purpose under NPP 2, then the organisation must take reasonable steps to destroy or permanently de-identify it,⁸ and
- NPP 2.1 provided that an organisation may only use or disclose personal information for the primary purpose of collection, unless an exception applies.⁹

Findings

Security of personal information (NPP 4.1)

In assessing whether Cupid took reasonable steps to comply with NPP 4.1, the Commissioner considered information from Cupid about the security safeguards in place prior to the data breach, and what steps would have been reasonable in the circumstances to protect the personal information held. This included considering Cupid's particular circumstances, such as:

- the volume and the sensitivity of the personal information it handled, and
- the likely impact in the event that the personal information was compromised.

The Commissioner also had regard to the guidance set out in the OAIC's *Guide to information security*.¹⁰

Nature of personal information

Cupid stated that as it does not store credit card information or bank account data, less stringent steps could be required of it than organisations that store financial or sensitive data.

⁶ See Privacy Act s 6D(4). A business with an annual turnover of less than \$3 million that trades in personal information is now covered by the APPs.

⁷ See APP 11.1 for current applicable APP.

⁸ See APP 11.2 for current applicable APP.

⁹ See APP 6.1 for current applicable APP.

¹⁰ www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-information-security.

However, the Commissioner noted that data other than credit and other financial information may be 'sensitive information' under the definition of that term in the Privacy Act.¹¹ Particularly, the Commissioner noted that Cupid offers services via sites categorised as 'African dating', 'Asian dating', 'Latin dating', 'gay and lesbian dating', 'special interest' and 'religion'. The personal information that Cupid handles in relation to user accounts for these particular sites will include 'sensitive information' for the purposes of the Privacy Act. The Commissioner therefore found that more stringent steps were required of Cupid to keep this information secure than may be required of organisations that do not handle sensitive information.

Information and patch management

Cupid advised that it uses information management tools, including the following:

- patch application and management, including processes to identify and install patches and security updates as they become available from Cupid's third party software suppliers
- antivirus software protection on all servers, including updates and maintenance, and
- database segregation (database information is kept on a separate network to website information, so that database information is only accessible by Cupid web servers and not the public internet).

Installation of malicious software (malware) detection and prevention software (including antivirus software) is a reasonably affordable security step that can assist organisations to prevent attacks by malicious hackers and the damage caused by malware.

Further, effective use of patches can assist organisations to fix system vulnerabilities and other problems. Had Cupid received an alert from the developer that the patch was available, but not applied the patch, the Commissioner may have considered there to have been a failure by Cupid to take reasonable security steps. However, as Cupid independently identified the patch and then applied it immediately, in the circumstances the Commissioner considered Cupid to have used patches effectively.

Separating an entity's network into multiple functional and informational segments makes it more difficult for an intruder to propagate inside the network. Segmentation can also allow for different security measures to be applied to different types of information depending on its sensitivity and the risks associated with it.

The Commissioner considered that the information and patch management steps taken by Cupid, including those above, were reasonable security steps for the purposes of NPP 4.1 in the circumstances.

Testing and monitoring

Cupid stated that it used the following testing and monitoring processes at the time of the data breach:

¹¹ See s 6 of the Privacy Act. Section 6 provides that 'sensitive information' includes information or an opinion about an individual's racial or ethnic origin, political opinions, religious beliefs, or sexual orientation or practices.

- daily vulnerability scans, and
- an intrusion prevention and intrusion detection firewall.

Intrusion detection systems, which use systems to monitor network or system activities for malicious activities and anomalous behaviour, can be an effective way of identifying and responding to known attack profiles.

On 21 January 2013, Cupid identified a rogue file on one of its servers, and that a hacker had attempted to gain access to a particular table within its databases. In response, Cupid took steps including applying the patch which fixed the vulnerability, which in turn stopped the attackers from obtaining further data.

In these circumstances, I am satisfied that the testing and monitoring steps taken by Cupid were reasonable steps as required by NPP 4.1.

Passwords and encryption

Cupid advised that it used the following password protection mechanisms at the time of the data breach:

- an account lockout policy, and
- enforcement of strong password policies on all servers.

Following the data breach, Cupid also promptly initiated a password reset process for all its users. This included encouraging users, as an extra security precaution, to reset passwords for different online services where the users used the same password as used for Cupid. The Commissioner considers password reset processes to be reasonable security steps and good privacy practise generally.

However the compromised passwords were not salted or hashed, or otherwise encrypted, before the data breach. Instead they were stored insecurely, in plain text.

Encryption strategies such as hashing and salting¹² are simple and effective means by which organisations can:

- securely store user passwords, and
- limit the risk of unauthorised parties gaining access to user accounts to which the passwords relate in the event the passwords are compromised.

Where passwords are hashed, it is also very difficult for attackers to recover the plain text version of the password (although the Commissioner acknowledged that tools are available to assist hackers with guessing passwords).

¹² 'Salting' is basically where an additional string of data, such as random numbers or text, is added to the password to make it less predictable and harder to attack, and 'hashing' is where passwords are processed through cryptographic algorithms that convert them into seemingly random characters. While passwords may be guessed through computational 'brute-force' attacks, this becomes very difficult when strong hash algorithms and passwords are used. Hashed passwords are therefore more secure to store than their clear-text passwords.

Password encryption strategies such as hashing and salting are basic security steps that were available to Cupid at the time of the data breach that may have prevented unauthorised access to user accounts. The Commissioner therefore found Cupid's storage of passwords in plain text to be a failure to take reasonable security steps for the purpose of NPP 4.1.

Secure destruction or permanent de-identification of personal information that is no longer required (NPP 4.2)

NPP 4.2 required organisations to take reasonable steps to destroy or permanently de-identify personal information that is not being used or disclosed for any purpose under NPP 2 (in other words, where the personal information is no longer required). To comply with this obligation, an organisation must have had systems or procedures in place to identify information the organisation no longer needed, and a process for how the destruction or de-identification of the information would occur.

Cupid advised that although the media had reported that 42 million users' accounts were compromised as a result of the data breach, this figure is not accurate because it includes 'junk' accounts and duplicate accounts. In other words, the personal information pertaining to a significant number of accounts was not in use by Cupid. Further, Cupid confirmed that at the time of the data breach, it did not have any particular systems in place to identify accounts that were no longer needed or in use, or a process for how the destruction or de-identification of personal information related to such accounts would occur.

Therefore, the Commissioner considered that prior to the data breach Cupid failed to take reasonable steps to destroy or permanently de-identify the personal information it held in relation to user accounts that were no longer in use or needed, in contravention of NPP 4.2.

Disclosure of personal information (NPP 2.1)

In general terms, an organisation discloses personal information when it releases information, whether purposely or accidentally, to others outside the organisation. This requires the organisation to release the information by its own action, intentionally or otherwise.¹³

In respect of the data breach, Cupid customer information was accessed as a result of a hacking attack, in which the attacker penetrated security features to access the personal information online. The Commissioner did not consider this to be a 'disclosure' by Cupid within the meaning of NPP 2.

Therefore, the Commissioner did not consider Cupid to have breached NPP 2 in this matter.

¹³ See 'Disclosure' section in Chapter B: Key concepts, APP Guidelines — http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-b-key-concepts#_Toc380575614.

Rectification

The Commissioner found that Cupid acted appropriately in responding to the data breach. Cupid identified that the ColdFusion vulnerability caused the data breach. Once the vulnerability was identified, Cupid immediately obtained and applied the patch released by the ColdFusion developer on all its servers to fix the vulnerability. Cupid also worked with an external ColdFusion security contractor to ensure the vulnerability had been successfully patched and that the then current ColdFusion installation met best practise standards.

Cupid then took the following ancillary steps to contain the data breach:

- sent a notification to all affected users with a valid email address, setting out that Cupid had experienced a data breach and automatically reset users' passwords (in the notification, as an extra security precaution, Cupid also encouraged users to reset passwords for different online services where they used the same password as used for their Cupid account)
- analysed server logs and tracked the hack method to ensure the breach had been contained
- conducted:
 - a full scan of all servers and removed all compromised files
 - a second scan of all servers using a specific rootkit detector, which confirmed that the malicious file was removed and that there were no other malicious files
 - a third scan of all servers using another type of rootkit detector which confirmed that there were no malicious files, and
- engaged a security team which conducted a full audit of Cupid's servers and confirmed that all threats had been removed.

Since the data breach, Cupid has undertaken an extensive privacy and data security remediation program, to ensure that it is APP compliant and to prevent attackers from accessing user data in the event that Cupid's website is hacked again. Particular measures include:

- development and implementation of a data breach response plan
- hashing of all user passwords with a unique salt
- implementation of daily hacking and vulnerability scans, with a focus on ColdFusion
- development of additional mechanisms for receiving timely notifications of security flaws, including through implementation of a monitoring program to identify software patches in the event that developers/vendors do not alert Cupid to patch availability
- review of best practise data storage methods for personal information
- conducting a review of personal information required to ensure Cupid is only collecting and retaining the personal information that is necessary

- procurement and installation of additional firewall security hardware
- development and implementation of rules to de-identify personal information relating to old or inactive user accounts, and
- engagement of privacy lawyers, whom have assisted Cupid to:
 - improve its processes generally for APP and Privacy Act compliance
 - revise its privacy policy and terms and conditions for APP and Privacy Act compliance, and
 - implement a number of other information security best practises.

Recommendations

The Commissioner found that the measures Cupid has taken in response to the data breach will assist Cupid to:

- significantly strengthen its privacy framework
- establish a privacy protective culture, and
- meet its obligations under Privacy Act and the APPs, which replaced the NPPs on 12 March 2014.

The Commissioner also recommended that Cupid regularly review its data security processes to continue to aim for best privacy practise that protects the personal information of its extensive user base.

Cupid did not notify the OAIC about the data breach. Notifying the OAIC can be a useful step in responding to a data breach,¹⁴ and the Commissioner encourages voluntary notification.

Conclusion

The Commissioner found that Cupid:

- failed to take reasonable steps to ensure the security of the personal information that it held, in contravention of NPP 4.1, and
- failed to take reasonable steps to destroy or permanently de-identify the personal information it held in contravention of NPP 4.2.

Cupid acted appropriately in response to the data breach including by:

- obtaining and applying a security patch to fix the vulnerability, and

¹⁴ An organisation's decision to notify the OAIC on its own initiative is likely to be viewed by the public as a positive action. It demonstrates that the agency or organisation views the protection of personal information as a serious matter, and may therefore enhance client/public confidence in the organisation.

- notifying affected individuals and ensuring they reset their passwords (and encouraging users to reset passwords for different online services where they used the same password as used for their Cupid account).

Cupid has also addressed the OAIC's recommendations, including by implementing a policy for determining when personal information is no longer required.

Based on the information from Cupid about its review and remediation of the data breach and Cupid's ongoing implementation of recommendations made by the OAIC, the Commissioner decided to close the investigation.

Acronyms and abbreviations

Commissioner — Australian Privacy Commissioner

NPPs — National Privacy Principles (contained in Schedule 3 of the *Privacy Act 1988* (Cth))

OAIC — Office of the Australian Information Commissioner

Privacy Act — *Privacy Act 1988* (Cth)