DLA PIPER

27 JULY 2014

LOVE IN THE TIME OF THE NPP

PRIVACY UPDATE

PRIVACY COMMISSIONER FINDS CUPID MEDIA IN BREACH

Earlier this week the Australian Privacy Commissioner found that Cupid Media Pty Ltd (**Cupid**), the operator of over 35 niche online dating websites, failed to take reasonable steps to secure personal information held on its websites and had therefore breached its obligations under the Privacy Act. The investigation was prompted by media allegations that the personal information of Cupid users, including full names, email addresses, passwords and dates of birth had been found on a server operated by hackers. The nature of the niche dating websites also meant that the hackers had access to sensitive information including users' sexual orientation, religious affiliations and racial and ethnic origins.

The **Privacy Commissioner's report** indicates that in January 2013 Cupid identified a rogue file on its servers. Cupid's investigations into the rogue file found that hackers had exploited a vulnerability in the application server platform which allowed them to access Cupid's databases. A patch for the vulnerability had been released days before the attack, however Cupid had not received notice from the developer that the patch was available (despite this being the usual practice). Cupid promptly applied the patch after becoming aware of its existence which prevented the hackers from obtaining further data.

At the time of the data security breach, the Australian Privacy Principles (**APPs**) were not yet in force. Accordingly, the Privacy Commissioner considered whether Cupid had complied with the following National Privacy Principles which required organisations:

- to take reasonable steps to protect the personal information they hold from misuse and loss and from unauthorised access, modification or disclosure (now covered by **APP 11.1**);
- to take reasonable steps to destroy or permanently de-identify personal information that they no longer need for any purpose for

which the information was collected (now covered by **APP 11.2**); and

- to use or disclose personal information only for the purposes identified at the time of collection, unless an exception applies (now covered by **APP 6.1**).

The Privacy Commissioner found that Cupid had taken a number of reasonable steps to protect the personal information (which included sensitive information such as racial/ethnic origin, religious beliefs or affiliations and sexual orientation) of its users. These steps included:

- applying patches and security updates as they became available from suppliers;
- utilising malware and antivirus software;
- utilising database segmentation techniques;
- conducting daily vulnerability scans; and
- operating an intrusion prevention and intrusion detection firewall.

However, Cupid stored user passwords in an insecure manner in plain text. The failure to apply encryption techniques such as hashing or salting to these passwords was enough for the Privacy Commissioner to find that Cupid had breached its first obligation.

The media allegations of the Cupid data breach reported that the personal information of 42 million users had been compromised. However, Cupid advised that there were a number of junk and duplicate accounts, meaning this figure was not accurate. Cupid had no process in place to identify unused accounts and subsequently destroy or de-identify the personal information contained in those accounts. Therefore, Cupid was also found to have breached its second obligation.

The final issue was whether Cupid had "disclosed" the personal information of its users through the cyber-attack. Importantly, the Privacy Commissioner noted that the concept of "disclosure" requires an entity to have "released the information by its own action, intentionally or otherwise". Therefore, an entity will not be considered to have disclosed personal information where a hacker accesses the personal information by penetrating security features.

Fortunately for Cupid, no financial penalty was imposed for these breaches. However this is most likely because of the rapid action taken to apply the patch and notify users of the breach as well as the level of cooperation provided to the Privacy Commissioner during the investigation.

ARE YOU SAFE?

The report is a timely reminder for businesses to ensure that they have implemented appropriate levels of security in relation to the personal information they have collected - particularly if that information is sensitive in nature. Furthermore, it is a reminder to schedule a "spring clean" and ensure that data that is no longer required is destroyed or permanently de-identified.

For more guidance about how to comply with your obligations to keep personal information secure and to destroy or de-identify personal information that is no longer required, please refer to our previous updates:

- Information security obligations for Australian business under the Privacy Act, and
- What do death, taxes and deactivated online accounts have in common?

FURTHER INFORMATION

For further information on any of the topics discussed, do not hesitate to contact:

Alec Christie
Partner
T +61 2 9286 8237
alec.christie@dlapiper.com

Jaimie Wolbers
Solicitor
T +61 2 9286 8022
jaimie.wolbers@dlapiper.com

Contact your nearest DLA Piper office:

BRISBANE

Level 28, Waterfront Place
1 Eagle Street
Brisbane QLD 4000
T +61 7 3246 4000
F +61 7 3229 4077
brisbane@dlapiper.com

CANBERRA

Level 3, 55 Wentworth Avenue
Kingston ACT 2604
T +61 2 6201 8787
F +61 2 6230 7848
canberra@dlapiper.com

MELBOURNE

Level 21, 140 William Street
Melbourne VIC 3000
T +61 3 9274 5000
F +61 3 9274 5111
melbourne@dlapiper.com

PERTH

Level 31, Central Park
152–158 St Georges Terrace
Perth WA 6000
T +61 8 6467 6000
F +61 8 6467 6001
perth@dlapiper.com

SYDNEY

Level 22, 1 Martin Place
Sydney NSW 2000
T +61 2 9286 8000
F +61 2 9286 8007
sydney@dlapiper.com

www.dlapiper.com

JAB/TAH/AUM/1206772709.1