CLIFFORD
CHANCE

Briefing note September 2016

Caught in the (Privacy) Act – The Ashley Madison data breach report

Ashley Madison, a website targeted at people seeking a discreet affair, is now widely known by the public for all the wrong reasons. One of these reasons is its failure to properly secure the personal information of its users. The company which owns Ashley Madison, Avid Life Media (ALM), whilst headquartered in Canada had users in more than 50 countries (including Australia) who engaged with Ashley Madison and ALM's other popular websites Established Men, Cougar Life and Man Crunch. The joint report of the Office of the Privacy Commissioner of Canada (OPC) and the Office of the Australian Information Commissioner (OAIC) into the breach provides important lessons for those concerned about user privacy.

What happened?

As has been publicised across the globe, in July 2015, a group called 'The Impact Team' announced that they had hacked ALM and threatened to expose the personal information of Ashley Madison users unless the site was shut down. ALM did not agree to this demand and reported the breach to the OPC. On 18 and 20 August 2015 The Impact Team published information, which included the account details of about 36 million Ashley Madison users.

Of the accounts released, there were more than one million Canadian users and about 670,000 Australian users affected. The OPC and the OAIC jointly investigated ALM's privacy practices and policies at the time of the data breach and also reviewed a number of related issues. The report prepared by the OPC and OAIC (Joint Report) provides great lessons for businesses, especially for those where user privacy (and secrecy) is at the core of their business.

What went wrong?

Under the Australian Privacy Act 1988 (Australian Privacy Act), the fundamental test for whether a contravention has occurred was whether ALM had taken such steps as were reasonable in the

Clifford Chance is the legal sponsor of Deloitte Technology Fast 50 Australia and is proud to support Australia's growing technology companies.

What we've learnt

- Beware! – any company doing business in Australia may be subject to the Australian privacy laws, even if it has no physical presence in Australia.
- Any business that holds personal information electronically must adopt clear and appropriate processes, procedures and systems to handle information security risks.
- When considering whether your processes, procedures and systems are adequate, consider the potential risk of harm to individuals from information being released.
- Be transparent with your users about the use of their information and be careful of representations your business makes about how securely their information is being held.

circumstances to protect the personal information it held. It's important to keep in mind that a data breach or other security compromise does not necessarily mean that there has been a contravention of either the Australian Privacy Act or the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA).

Process, procedures and systems

The primary lesson from the Joint Report is that it's crucial for any business that holds personal information electronically to adopt clear and appropriate processes, procedures and systems to handle information security risks, supported by adequate expertise (internal or external), particularly where the information is sensitive or could cause significant harm to the individuals affected.

When assessing what are reasonable processes, procedures and systems a company should consider the potential risk of harm to individuals from the release of the information. In some circumstances the release of a name or an email address may not in itself be harmful but in the case of Ashley Madison, the association of such basic information with the website was enough to cause reputational harm to users.

Key missing features

The Commissioners identified three key elements that ALM's security framework was lacking:

1. Documented information security policies or practices, including appropriate training, resourcing and management focus;
2. An explicit risk management process - including periodic and pro-active assessments of privacy threats, and evaluations of security practices to ensure ALM's security arrangements were, and remained, fit for purpose; and
3. Adequate training to ensure all staff (including senior management) were aware of, and properly carried out, their privacy and security obligations appropriate to their role and the nature of ALM's business.

What should you look out for?

In addition to the key elements identified above, the Joint Report makes a number of observations with respect to the particular circumstances in the Ashley Madison data breach.

- **Trust marks**: At the time of the breach the Ashley Madison website had a number of trust marks which conveyed general impression that the website adhered to a high level of security. Given the nature of information and the impression conveyed by these marks, the level of security safeguards actually in place should have been commensurately high. Examples include the "SSL Secure Site" graphic, "100% Discreet Service" and "Trusted Security Award".
- **Indefinite retention and "Pay for Privacy"**: ALM had a policy of indefinitely retaining information and a premium "Pay for Privacy" service which forced users to pay to permanently delete their profiles. Neither of these were considered acceptable under the Australian Privacy Act.
- **Accuracy of email addresses**: ALM's lack of systems for verifying whether an email address was real and associated with an actual user of Ashley Madison, exposed potential non-users to reputational harm (famously in the case of NZ Prime Minister John Key, a fake email address john.key@pm.govt.nz was registered).
- **Transparency with users**: ALM failed in a number of instances to obtain their users fully informed consent. For example, users were not notified until after registration that they could not delete their account without paying a fee and further, only after paying for the deletion were informed that their information would be kept for 6-12 months for chargeback purposes.

But we're not in Australia…

Whilst ALM is headquartered in Canada, it is subject to the Australian Privacy Act because it carries on business in Australia through its marketing in Australia and targets its services to Australian residents.

It is also subject to the Australian Privacy Act because it collected information from individuals physically located in Australia at the time of the data breach.

This extraterritoriality of the Australian Privacy Act has significant implications for the risk management of any company transacting and doing business in Australia (especially technology businesses) or collecting personal information from people located in Australia.

Who should be notified?

The Australian Federal Government is currently considering legislation creating a serious data breach mandatory notification regime. The draft bill imposes on regulated entities an obligation to notify the OAIC of a 'serious data breach' and take such steps as are reasonable to notify the individuals affected by the serious data breach of the incident or if not practicable, publish a copy of the statement provided to the Commissioner on its website and publicise the contents of the statement.

Given the extraterritorial reach of the Australian Privacy Act, non-Australian entities, like ALM may become subject to the mandatory data breach reporting. Further, once published such information will inevitably lead to pressure to report breaches in other relevant jurisdictions, even if there is no legal obligations to do so in those jurisdictions.

What happens next?

ALM have agreed to address the concerns of the Joint Report. Some of the undertakings are set out below.

- conduct a comprehensive review of protections in place for information;
- undertake steps to ensure staff are aware of and follow security procedures, which will include an appropriate training program;
- provide the OAIC with a report from an independent third party documenting the measures taken;
- cease its practice of indefinite retention of information; and
- amend its account creation process to ensure accuracy of information.

Importantly, ALM have undertaken to confirm in writing to the OAIC its implementation of each undertaking and to provide all documents and information that may be requested by the OAIC. The OAIC will be monitoring closely!

Collateral consequences

It has been recently reported in the Financial Times that a British cyber security firm has searched through data from recent breaches of popular websites, including Ashley Madison.

The firm found that Ashley Madison alone yielded corporate emails and passwords of more than 200,000 people working for big companies. It was reported that in many instances work passwords were reused. This creates an additional security threat for companies and a need to focus on security from a cultural perspective.

Contacts

Sydney

Lance Sacks
Partner
T: +61 2 8922 8005
E: lance.sacks@cliffordchance.com

Jerrem Ng
Senior Associate
T: +61 2 8922 8069
E: jerrem.ng@cliffordchance.com

James Kwong
Graduate Lawyer
T: +61 2 8922 8084
E: james.kwong@cliffordchance.com

Perth

Justin Harris
Partner
T: +61 8 9262 5503
E: justin.harris@cliffordchance.com

Shane Stewart
Senior Associate
T: +61 8 9262 5507
E: shane.stewart@cliffordchance.com