Data breaches: Your iPhone and the damage done

The *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth), the application and risk to law firms

back to contents

Christine Smyth and **Shane Budden** discuss the impact of new federal privacy legislation and how firms will need to be proactive in their responses.

It's been a long day, finalising that brief was a total punish. Exhausted, all you want to do is head home, but no, you now have a work function to attend.

You take a deep breath, put on the battle jacket and head off. At 11pm you finally make it home, pay the cabbie and in your overtired, dreary state, climb out of the car, onto your doorstep fumbling for your keys, and collapse gratefully into bed.

You wake late the next morning, wondering why your alarm didn't go off – only to realise that it probably did, but you didn't hear it because you left your phone in the back of the cab.

You think to yourself, it's annoying, but it's not that bad, it's a simple matter of reporting it to work and applying for a new phone, right?

Wrong. For the average punter that might be the case, but as a solicitor that lost phone has just thrown you into the maelstrom that is the *Privacy Amendment (Notifiable Data Breaches) Act 2017* which commenced on 22 February 2018.

You haven't just lost a phone, you've lost client data – which may be a notifiable data breach – one that must be reported to any clients affected and the Australian Information Commissioner. Failure to do so can result in crippling fines.

To whom does the scheme apply?

The scheme is implemented via an amendment to the *Privacy Act 1988* (Cth) which inserts a new part: *IIIC—Notification of Eligible Data Breaches.*

The scheme applies to Australian Privacy Principles (APP) entities as defined in the *Privacy Act 1988*, which includes businesses with turnover of $3 million or more in any financial year since 2001.[1]

While many law firms do not have turnover of $3 million or more, on the commencement of the anti-money laundering legislation, all law firms must comply. In addition, for the purposes of part IIIC, the definition of *entity* includes a person who is a tax file number recipient[2] meaning that any firm which receives the tax file numbers of clients may be caught by the scheme.[3]

In practical terms, prudent practitioners will operate as if the scheme applies to them.

What is an eligible data breach?

26WE defines an eligible data breach as being unauthorised access to information, or loss of information, where unauthorised access is likely, where the information involved is such that a reasonable person would conclude that access is likely to result in serious harm to any of the individuals to whom the information relates.

Although the drafting is clumsy, the practical message is simple: law firms holding personal information must take measures to secure that information.

What is serious harm?

Section 26WG considers the question of serious harm, by providing the factors which may be taken into account when deciding the issue. Those factors include the nature of the information, whether or not it is protected by security (for example, a locked iPhone or password-protected USB) and, if so, the likelihood of that security being defeated, and whether or not the information was encrypted (and again, the strength of that encryption).

These factors also include an assessment of the persons who have obtained (or are likely to obtain) the information, and whether or not they are likely to defeat any security/encryption measures.

The nature of the harm can also be taken into account, but this gives little comfort; given the many ways in which personal information can now be used to perpetrate fraud and steal money and other information, it is difficult to imagine circumstances in which the potential harm could not be defined as 'serious'.

In the lost phone scenario, it is worth noting that the protections on certain phones, such as iPhones and Blackberrys, have historically proven remarkably resistant to compromise, but that may not remain the case.

What action must be taken?

If a law firm becomes aware that there are reasonable grounds to suspect that there may have been an eligible data breach, section 26WH provides that it must expeditiously carry out an assessment as to whether or not that is the case, and must take all reasonable steps to do so within 30 days. If the conclusion reached is that there are reasonable grounds to believe that there has been an eligible data breach, the process in section 26WK must be followed.

In that case, as soon as practicable after the breach/potential breach has been detected, a statement must be prepared – and sent to the Commissioner – which includes the following information:

- the identity and contact details for the firm
- a description of the breach
- the kind of information that is the subject of the breach
- the steps that individuals affected by the breach should take.

As soon as is practicable after the completion of the statement, pursuant to s26WL the firm must (if practicable):

- take reasonable steps to notify the contents of the statement to each of the individuals to whom the relevant information relates, or
- take reasonable steps to notify the contents of the statement to each of the individuals who are at risk from the data breach.

back to contents

If neither of these actions is practicable, the firm must publish the statement on its website and take reasonable steps to publicise its contents.

Are there exceptions?

There are limited circumstances in which a data breach need not be reported, although practitioners should consider the situation thoroughly before deciding that no further action need be taken; the consequences of misapplying exceptions could be disastrous.

The exception most pertinent to the operation of a law firm is that provided for if remedial action is taken. S26WF (1) provides an exception if access to, or disclosure of, information to which this Act applies, providing the entity:

- takes remedial action
- the action is taken before serious harm is done, and
- the action is taken soon enough that a reasonable person would conclude serious harm was unlikely to occur.

If those criteria are fulfilled, the disclosure is taken never to have been an eligible data breach. In our scenario above, for example, if the lost phone was remotely deleted before anyone managed to access it, it is likely no breach would have occurred.

Several other exemptions are allowed in the legislation, which are more likely to relate to client breaches than law firm breaches. A detailed consideration of these exceptions is beyond the scope of this article, but in short compass they are as follows:

- *Enforcement related activities*: s26WN provides a general exception if compliance with the reporting provisions of the part would prejudice one or more enforcement-related activities conducted by, or on behalf of, the enforcement body.
- *Inconsistency with secrecy provisions*: s26WP provides a general exception if compliance with the reporting provisions of the part would, to any extent, be inconsistent with a secrecy provision (other than a prescribed secrecy provision).
- *Declaration by Commissioner*: s26WQ gives the Commissioner power to declare that ss26WK and s26WL do not apply to a given breach, or to extend time for compliance with s26WL.
- *My Health Records Act 2012*: s26WD provides an exception if a breach has been, or is required to be, notified under section 75 of the *My Health Records Act 2012*.

What are the consequences of failing to act?

Failure to comply with the new regime will be considered an interference with the privacy of an individual. A law firm which is found to have done this will be liable to significant penalties, including fines of up to $2.1 million. Such fines would be terminal for many law firms, which underscores the importance of understanding and complying with the reporting regime.

Prudent preventative actions

Few practice risks lend themselves as readily to the mantra 'prevention is better than cure' than the data breach reporting regime, and practitioners must be proactive in addressing this risk. The following suggestions are not a panacea but may assist in reducing the risk of a notifiable breach.

- *Deliberate disclosure*: If a client wishes you to disclose personal information, ensure that consent to do so is informed and in writing.

- *Staff procedures*: Detailed and robust staff procedures – and training in those procedures – should be implemented around data security, including taking data off-site in storage devices.
- *Remote deletion*: Electronic devices such as phones and laptops should allow remote deletion if lost/stolen.
- *Use of USBs*: If staff are to store client data on USBs and take them off-site, those USBs should be encrypted. In addition, the firm should provide the USBs, keep a register of them – and what data is on them – and have them signed in and out to ensure their whereabouts are always known.
- *Brand electronic devices:* All work devices and property capable of data storage should carry the firm name and contact details, to ensure they can be easily returned if found.
- *Routines/checklists*: Develop and utilise mental checklists to go through when leaving areas such as hotel rooms or boarding lounges (for example, before boarding a plane, check off boarding pass, wallet, home phone, work phone).

As no prevention regime is foolproof, also ensure that you have a data breach response plan in place, and that staff are aware of it.

It is beyond the scope of this article to cover such a plan, but useful assistance can be found in the privacy law section of the Office of the Australian Information Commissioner (OAIC) website at **oaic.gov.au**.

Conclusion

Data breaches *are not* an IT issue; they are a process and procedure issue, and one which will affect large numbers of law practices.

We stand at a time of fundamental change to the way we do business; the value of client data and private information – and the damage that can flow from disclosure – means that, regardless of size, turnover and resources, law firms will be expected to provide high levels of data security and comply with strict standards in relation to data management.

In the United States, a growth industry in auditing and ranking the cyber-security measures of law firms has sprung up almost overnight, with savvy clients now insisting on a certain rating being achieved before doing business. We can expect a similar system to evolve here. Data security is quite literally an existential issue for law firms.

Not since the implementation of practice management qualifications in the 1980s have we seen such a seismic shift in the way practices are managed, and no doubt more is on the way.

This scheme, and the anti-money laundering regimes, are the tip of the iceberg, and practitioners can be certain that the bar on what constitutes best practice will be raised in many areas. The time to get on top of these issues is now. And be careful not to throw out filing cabinets before checking that they are empty.

Christine Smyth is immediate past president of Queensland Law Society and partner at Robbins Watson Solicitors. Shane Budden is an ethics solicitor at the QLS Ethics Centre.

Notes

[1] ss6C and 6D *Privacy Act 1988* (Cth).
[2] s26 WB *Privacy Act 1988* (Cth).
[3] s26WE (1)(d) *Privacy Act 1988* (Cth).