# Does the law in Australasia support organisations archiving their email databases on the cloud?

April 2017

**Speed read**

Archiving emails with cloud providers brings benefits such as cost efficiencies, searchability, and (potentially) better security and reliability. Privacy and cybersecurity law applicable to Australian and NZ organisations permits this, so long as particular requirements are met. However, there will be some sector specific legal requirements that affect the ability to benefit from cloud archiving.

Transferring the data to off-shore cloud locations is a particular issue to consider.

Michael Wigley presented this paper originally at a webinar hosted by CIO 'Cloud Archiving: The Road to Simplified Data Retention'.

**The Detail**

Public and private sector organisations with large databases of emails to be archived, are increasingly looking at archiving in the cloud. That replaces, typically, archiving on the organisation's own servers and storage.

This has some real benefits for those organisations, such as:

- Storage and administration cost efficiencies and other benefits;
- Searchability, with the email database in one place not mulitple;
- Better security (perhaps, but in all this, it depends on the specifics);
- e-Discovery efficiencies;
- remote/mobile access;
- reliability

But what is the legal position as to archiving on the cloud, given that the organisation will often outsource the storage to cloud providers with servers offshore? We'll address general obligations and then move to off-shore specific obligations, setting out the Australian and NZ position in separate boxes (but in practice there is not a great deal of difference).

To the fore are cybersecurity and privacy/ confidentiality legal issues.

**Health warning**

We address the general position here, but there are contract, industry and legislation specific issues in particular sectors. For example, the public sector has specific legislation and guidelines; the finance sector has specific legislation and guidelines;[1] and so on. This illustrates a key point: it is necessary to check the specifics in each organisation.

One risk area is that contracts with say suppliers or customers can promise the unachievable - 100% security and safety, or similar - when that is not available in the real world. In any cybersecurity assessment, that is an important area to check and fix.

**Some general legal principles; industry guidelines and best practice**

Organisations have been outsourcing to cloud providers for years now, and in most respects, archiving emails on the cloud is largely doing the same.

Broadly, the organisation must take reasonable care, in the circumstances, to ensure the information is protected. That duty still

Does the law in Australasia support organisations archiving their email databases on the cloud?

largely lies with the organisation when there is outsourcing to a cloud provider. The organisation can't just say: "*It's their responsibility now, not ours*".

The sources of these obligations are not just the Privacy Act. They include:

- Tort (e.g. liability for negligence, and, depending on the country, tort relating to privacy);
- Equitable or other duties of confidentiality
- Contract as noted above;
- Specific statutes

Something of a common theme through the above (but subject to specific circumstances) is that organisations should take reasonable care as to protecting data and cybersecurity. That is a theme of the Privacy Acts and of the law of negligence for example. This often translates into meeting industry guidelines and best practice. That also helps reduce other risks such as reputational risk.

Thus, organisations reduce legal and other risks by implementing up to date industry best practice.

Some specifics on the Privacy Acts:

**Australia**

APP 11 Privacy Act requires an APP entity to take active measures to ensure the security of personal information it holds, and to actively consider whether it is permitted to retain personal information. **An APP entity that holds personal information must take reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure.**

**New Zealand**

IPP5 Privacy Act provides (bold added):

Storage and security of personal information

An agency that holds personal information shall ensure—

(a) that the information is protected, by such security safeguards **as it is reasonable in the circumstances to take,** against—

- loss; and
- access, use, modification, or disclosure, except with the authority of the agency that holds the information; and
- other misuse; and

(b) that **if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.**

**Off shore concerns**

Assuming no industry or sector specific concerns, both NZ and Australia[2] permit off shore cloud hosting of information such as emails. But, as outlined above, the organisation cannot just leave it to the off-shore host, for it retains much responsibility. A topical illustration is that the organisation retains the disclosure obligation under the new Australian Mandatory Breach Reporting regime if there is a breach by the offshore provider.

Additionally, the way in which the emails are held and accessed may impact the legal obligations: the points in the box below as to Australia illustrates this.

Therefore, the organisation should vet and monitor what is happening.

Here are some specifics about the Privacy Acts, in the way they apply to off shore transfer and holding of information by cloud providers:

**Australia**

APP11 in the Privacy Act, summarised above, applies in any event to emails archived and hosted with off-shore cloud providers.

The new mandatory data breach notification regime (under the Privacy Amendment (Notifiable Data Breaches) Act 2017) illustrates this. Where there is a data breach at the offshore cloud provider that would be notifiable if in Australia, the Australian company that contracted the cloud provider has a duty to notify (new s26WC).

Does the law in Australasia support organisations archiving their email databases on the cloud?

There is a specific regime in the Privacy Act applying where personal information is transferred offshore: that is APP8. Broadly, and there are some exceptions and detailed aspects, an organisation **disclosing** personal information offshore, must take steps to ensure the overseas recipient does not breach all APPs but APP1. That does not apply if there is informed consent from the person concerned, or the recipient is subject to privacy law as strong as the Australian Privacy Act. "Disclosure" does not include "use" where it may be that "use" means just holding the data on the part of the cloud provider (and duties don't arise where there is just "use". The dividing line between "disclosure" and "use" is vexed and depends on access rights, contracts, technology and so on. This may be angels dancing on the head of a pin overlapping. As the Privacy Commissioner has said:

> *"…the OAIC recognises that in some instances, it can be difficult to determine whether the information is being 'used', or whether it is being 'disclosed'. In such cases, the practical effect of distinguishing a 'use' from a 'disclosure' should not be overstated. Whether an APP entity sends personal information to an overseas recipient as a 'use' or as a 'disclosure', it may still be held accountable for mishandling of that information by the overseas recipient. In practice, the steps that an APP entity takes and their accountability when sending personal information overseas can be similar regardless of whether the information is being used or disclosed. For this reason, where it is unclear whether the personal information is being used or disclosed, the best approach is to take reasonable steps to ensure the APP are complied with. An APP entity that sends personal information overseas may be liable if the personal information is mishandled."*

**New Zealand**

IPP5(2) of the Privacy Act, quoted above, extends to a NZ agency providing personal information to a cloud provider where that data is hosted offshore. Therefore, the agency retains responsibility to ensure that *"everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information."*

Thus, NZ agencies should review and be satisfied with contracts with cloud providers, their technology and their security including as to getting the information back from them when needed. They should monitor this, particularly when the information moves to the more sensitive end of confidentiality.

**The laws in other countries**

Offshore archiving of documents, depending on the location where the information is located, accessible etc, may raise legal issues in other countries to be considered too. This may need to be checked.

**Conclusion**

Getting cybersecurity right, including archiving emails in the cloud, is a team exercise: IT; HR; CFO, CEO, legal; and so on.

[1] For example, see Peter Leonard, Gilbert & Tobin "Finding Clarity in the Clouds - Australian Privacy and Prudential Compliance of Cloud Services for Australian Business and Government Agencies" (Sep 2016)

[2] For more about the impact of Australia's Privacy Act, see Peter Leonard, Gilbert & Tobin "Australia's unique approach to trans-border privacy and cloud computing" (Aug 2015)

**Wigley**+Company
PO Box 10842
Level6/23 Waring Taylor Street, Wellington
T +64(4) 472 3023 E info@wigleylaw.com
and in Auckland
T +64(9) 307 5957
www.wigleylaw.com