NEW ZEALAND LAW SOCIETY

NZLS EST 1869

PRACTICE BRIEFING

Cloud Computing Guidelines for Lawyers

INTRODUCTION

Legal practices are increasingly using cloud storage and software systems as an alternative to in-house data storage and IT programmes.

The cloud has a number of advantages – particularly flexibility and cost – but these have to be balanced with risks to privacy and control.

The Lawyers and Conveyancers Act (Lawyers: Conduct and Client Care) Rules 2008 and the Privacy Act 1993 require lawyers to protect and hold in strict confidence all information concerning a client acquired in the course of the professional relationship.

This Practice Briefing aims to give Law Society members helpful guidance on best practices for moving to the cloud. It examines how cloud computing can be used while maintaining lawyers' professional obligations.

It is not intended to endorse cloud computing, to be legal advice, or an industry standard nor does it provide a defence to misconduct or improper professional practice.

PROFESSIONAL STANDARDS

Lawyers need to be aware of their obligations to protect clients' personal data. Any move to using cloud services cannot compromise these statutory obligations.

All use of cloud computing by lawyers and law firms must always be within the parameters of lawyers' professional obligations under the Rules of Conduct and Client Care and the Privacy Act 1993. These pieces of legislation outline requirements for lawyers when dealing with client personal information.

Guidance on the obligations lawyers have to protect clients' personal information in line with these two acts is available in another Law Society Practice Briefing, Protecting Clients' Personal Information

https://www.lawsociety.org.nz/practice-resources/practice-briefings/Protecting-clients-personal-information-2014-06-19-v1.pdf

NEW ZEALAND LAW SOCIETY

NZLS EST 1869

Lawyers' professional obligations to consider when outsourcing data storage

Chapters 8 and 11 of the Rules of Conduct and Client Care outline lawyers' fundamental obligations in protecting confidentiality.

Chapter 8 states the confidential information requirements:

- A lawyer has a duty to protect and to hold in strict confidence all information concerning a client, the retainer, and the client's business and affairs acquired in the course of the professional relationship.
- The obligation of confidentiality continues indefinitely after the person has ceased to be the lawyers' client.

Chapter 11 states the requirements for professional dealings:

- A lawyer's practice must be administered in a manner that ensures that the duties to the court and existing prospective, and former clients are adhered to, and that the reputation of the legal profession is preserved.
- A lawyer must take all reasonable steps to prevent any person perpetrating a crime or fraud through the lawyer's practice. (This includes taking reasonable steps to ensure the security of and access to electronic systems and passwords).

Adopting a third party cloud computing platform is likely to constitute outsourcing an operational function that could make it possible for that third party to access your clients' data.

It follows that you should seek contractual terms from your cloud supplier that would enable you to ensure:

- clients' information is protected and the cloud service will not compromise client confidentiality;
- that the law firm makes all reasonable efforts to ensure that hackers and cyber criminals cannot access client data when it is placed on the cloud.

To do this you need to understand the different layers of ownership and management in the arrangements.

These are clearly outlined in the United States' National institute of Standards and Technology (NIST) definition of Cloud Computing below.

Protecting clients' personal information

As laid out in the Practice Briefing Protecting Clients' Personal Information, it is advised that lawyers and firms have personal information protection policies in place.

The starting point for evaluating cloud services should be your practice's existing policies.

Informing clients' of third party storage of personal information

Under Information Privacy Principle 3 (section 6 The Privacy Act 1993) an agency must provide the name and address of the agency that will hold a client's personal information.

Clients should be informed when their confidential information is to be held or stored with any third party and directly authorise the third party to store their personal information.

Office of the Privacy Commissioner's guidance

The Office of the Privacy Commissioner has published general guidance for small business moving to the cloud, frequently referred to in this Practice Briefing, available online here:

www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/OPC-Cloud-Computing-guidance-February-2013.pdf

WHAT IS CLOUD COMPUTING?

This Practice Briefing uses the NIST definition of cloud computing.

NIST Definition

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Essential Characteristics:

On-demand self-service

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (for example, mobile phones, tablets, laptops, and workstations).

Resource pooling

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (eg, country, state, or datacentre). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at a time.

Measured success

Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (eg, storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilised service.

Service models

Software as a Service (SaaS)

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure.

The applications are accessible from various client devices through either a thin client interface, such as a web browser (eg,.web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user – specific application configuration settings.

Platform as a Service (PaaS)

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.

The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application – hosting environment.

Infrastructure as a Service (IaaS)

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (eg, host firewalls).

Deployment models

Private cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising

multiple consumers (eg, business units). It may be owned, managed, and operated by the organisation, a third party, or some combination of them, and it may exist on or off premises.

Community cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organisations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organisations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardised or proprietary technology that enables data and application portability (eg, cloud-bursting for load balancing between clouds).

Cloud computing examples

Amazon is an example of Infrastructure as a Service, and Platform as a Service. It allows users to operate databases and virtual servers.

Google Drive is an example of Software as a Service suite of ready-made applications – word processing, spreadsheets, databases and file storage. Through using Google Drive a consumer creates data which is then stored in Google's data centres.

There are also numerous specialist cloud services. **XERO**, for example, pioneered a cloud-based accounting service.

Cloud storage does not have to be based overseas. There are a variety of **New Zealand-owned cloud storage providers** with servers located in New Zealand.

MEETING YOUR IT NEEDS

Initially it is important to assess your business's IT needs, priorities and long term plan. For instance:

- What do you want your systems to do for you?
- Do your storage needs fluctuate?
- Do you need to be able to access your server/servers from multiple locations and multiple devices?
- What do your clients expect when they trust you with their personal information?

Below is a summary of the commonly cited benefits and risks associated with cloud computing. This list is indicative and not comprehensive.

Cloud computing benefits

- improved backup/disaster recovery;
- flexibility and agility;
- increased storage capacity;
- increased data handling capacity;
- reduced infrastructure costs;
- avoiding frequent updates to software;
- reduced internal IT staff costs;
- economies of scale;
- potentially more secure due to more expert staffing;
- better quality servers.

Cloud computing risks

- security;
- privacy breaches;
- cross-border privacy legislation;
- service reliability and stability;
- lack of control over customisation and integration;
- customer service;
- speed and bandwidth;
- danger of supplier lock-in;
- difficulty achieving executive buy-in;
- client insecure about privacy risks.

Approved ways to store data

The Practice Briefing Protecting Clients' Personal Information outlines best practice for storing personal information.

Part of this process is to label data and information stored in your organisation on a spectrum from high risk through to low risk. The degree of risk of this data should have storage correlations. A firm may decide that high risk data will be stored in a different way to low risk data.

It is important that the process is clear around storage of data and that staff do not use their own free cloud service-provided emails or storage facilities to transport high risk data.

For instance, a staff member should not be permitted to use their personal Gmail or Hotmail

email accounts to store confidential information so they can work remotely.

As outlined, policies should be clear and enforced so the employer is doing the best they can to ensure best practice is followed.

CLOUD COMPUTING CONTRACT CONSIDERATIONS

Cloud computing contracts vary widely. A good starting point is a comprehensive study by Shelston IP partner Mark Vincent, Cloud Computing in 2013 – What legal commitments can you expect from your provider. Looking at Australian providers, it showed the massive range of cloud computing contracts where some were in line with Australian Privacy standards, while others were far from it.

See *Cloud Computing Contracts – What Legal Commitments Can You Expect From Your Provider...* by Katrina Crooks, Shelston IP

Cloud computing contract negotiation

It used to be that service providers called all the shots; however, in an increasingly competitive market some cloud computing providers are willing to adapt their terms and conditions for big clients.

Small New Zealand cloud service providers may be willing to tailor a service to fit your needs, but these providers may not offer the financial and technology security of the bigger but less transparent or negotiable service providers.

Lawyers and firms thinking about moving to the cloud must go in with a clear understanding of their priorities and make risk evaluations in line with business goals.

Service provider reliability

The tech industry attracts some fly-by-night providers. When choosing a cloud provider it is extremely important that you look closely at the providers for:

- track record and reputation;
- commitment to the cloud computing market;
- existing customers;
- financial position, provisions in place if company goes bankrupt;
- what will happen to your data if things go wrong.

In any contractual agreement it is important to be thorough. Cloud computing offers a unique range of risks.

Here are some of the risks lawyers need to be particularly aware of in a cloud context.

Service level agreements

The Katrina Crooks report outlines that contracts concerning cloud service availability are most commonly governed by service level agreements (SLAs) which often provide a guarantee of the

percentage of time for which the service will be operational.

The remedy for failure to meet the guarantee is typically a service credit provided to the customer to offset fees for the month in question.

However, some down time was often not included in that calculation. This included scheduled maintenance; force majeure events; outage resulting from misuse of the service; and outages elsewhere on the Internet.

Some included an exorbitant list of down-time excuses.

SLAs must be scrutinised carefully to determine their overall effect and so that customers are aware of the requirements to be met in order to seek service credits. And that these are reasonable.

The Law Society of England and Wales recommends that lawyers consider various aspects of service availability, including:

- **point of measurement:** availability of service provision or availability at the point of user consumption;
- **service measurement period:** even if a service boasts high availability 24/7, this could translate into relatively high downtime during normal working hours;
- **application availability:** availability of particular applications may be just as important to you as general availability of a service.

The Law Society of England and Wales also recommends weighing up the relative merits of a credit regime against damages at common law and to be careful before accepting that service credits are your sole and exclusive remedy. This will limit the right to sue for damages at large or terminate the contract.

Service changes

You should ensure:

- that the company is contractually obligated to inform you of any structural changes to the business in advance;
- that you are able to terminate your contract under ownership changes;
- that your data cannot be held in receivership;
- that contracts can't be changed without informing you and giving you the right to terminate the contract;
- that the provider cannot suspend service without prior notice, agreement, and good faith – unless in specific circumstances, for instance, non-payment.

Subcontractors

Make sure you are aware where your data will journey at all times, and that your provider and (if relevant) subcontractors can't access your clients' data. You should also be clear on the rules surrounding subcontracting – whether it is permissible and what your involvement should be in the process.

Commercial gain

Some cloud providers sell data to third parties. You need to take precautions that your provider will not access or sell your data.

LOCATION OF DATA

Lawyers should be aware of where their data is located and the privacy laws in the jurisdiction where their data is being stored.

If the cloud service provider is unwilling to tell you the exact location of their data storage facilities, they need to be able to provide evidence of binding contractual commitments they have made to keep data in locations which won't compromise the privacy of their customers.

Examples are the European Union's Binding Corporate Rules and the Asia Pacific Economic Co-operation Cross Border Privacy Rules or, locally, CloudCode, administered by the New Zealand Institute of IT Professionals, offers best practice cloud providers the ability to become signatories.

More about CloudCode is online here: *www.thecloudcode.org*

Data location checklist

The Office of the Privacy Commissioner's guidance note Cloud Computing – A guide to making the right choices recommends that the following location information is sought from a cloud computing provider:

- whether there is a privacy law that applies in the country or countries where your data is stored or processed;
- whether that privacy law is similar to New Zealand's privacy law;
- whether the law applies to the cloud provider and to your information (some privacy laws exempt some types of businesses, or do not apply to the personal information of foreigners);
- how the cloud provider will deal with any requests for information that it receives from government agencies, courts etc. For example will the provider only disclose information in response to a court order?

Will the provider let you know if it has to disclose information in response to a request?;

- will the cloud provider notify you if data is lost or stolen, for instance if the provider is hacked?;
- who can you or your clients complain to if there's a breach of privacy?

Lawful third party access to data

International and domestic police or intelligence agencies can in certain circumstances lawfully obtain access to your data via your cloud service provider.

However, it is important to remember, there are also times when international and domestic

police or intelligence agencies can legally access data stored on your own server.

It is important to research the systems that a cloud service provider uses to deal with requests for information from government agencies and how they validate the legality of the requests. You should have a clear understanding with appropriate contractual and operational process in place to cover how the cloud service provider will deal with a request to access your data.

If a lawyer has concerns in respect of a certain client or class of client in respect of potential jurisdictional, privilege and third party access issues that may be a matter requiring serious consideration before choosing to store client info in the cloud.

GETTING DATA OUT

The New Zealand Privacy Commissioner's Cloud Computing guidance section "Where are the exits?" states that you need to be able to get your information out and make sure it's no longer retained on the provider's servers once you're gone.

The provider should state:

- whether you can take the information with you if you choose not to use the service any longer;
- whether the information will be returned in a format that you can use elsewhere – and the timeframes it will be returned in;
- who will bear the cost for the process of switching to a new supplier;
- whether information will be kept on the provider's systems after you move on, or whether it will be securely deleted. For instance, many providers will hold backups. which will keep records for a certain period even once an account is deleted;
- how the provider will verify for you that the information has been deleted.

The guidance note can be found online here: *https://privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/OPC-Cloud-Computing-guidance-February-2013.pdf*

VIRUSES, HACKERS AND OTHER CRIMINAL MATTERS

Chapter 11 of the Rules of Conduct and Client Care states that:

A lawyer must take all reasonable steps to prevent any person perpetrating a crime or fraud through the lawyer's practice. (This includes taking reasonable steps to ensure the security of and access to electronic systems and passwords).

International NGO the Cloud Security Alliance has put together a helpful matrix of cloud controls to assist organisations to determine whether their cloud service provider is providing adequate security. This is available here: *https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3/*

NEW ZEALAND LAW SOCIETY

NZLS EST 1869

GENERAL CHECKLIST

- Different cloud services carry different risks and responsibilities. How secure is your current system with handling personal information. Would it be safer stored with a trustworthy cloud provider?
- Encrypt data so it is protected both while it travels and when it's at the provider's end. Make sure your client's data will not be seen by any third parties.
- Research your provider thoroughly, online and via contacts. Read and compare providers' terms and conditions.
- See what legal jurisdiction's privacy laws a cloud provider operates under and what/if any non-government standards they have committed to.
- Know where your data is going to be stored and what privacy laws apply.
- Ask how you will be informed if your data has been compromised and what the protocols around this are.

Information in the Practice Briefing series is provided by the Law Society as a service to members. This briefing is intended to provide guidance and information on best practices. Some of the information and requirements may change over time and should be checked before any action is taken.

- A cloud provider should use third party auditors to ensure compliance.
- Ability to exit: can you delete information and easily take it with you to another provider if you choose to.
- Check what will happen to your data if the business goes bankrupt.
- Remember that you are responsible if your client's privacy is breached.

This list is based on the Office of the Privacy Commissioner's Cloud computing checklist for small business available online here: *http://www.privacy.org.nz/news-and-publications/guidance-notes/using-the-cloud/cloud-computing-checklist-for-small-business/*

NEW ZEALAND LAW SOCIETY
Law Society Building
26 Waring Taylor Street
WELLINGTON 6011

PO Box 5041
Lambton Quay
WELLINGTON 6145

(04) 472 7837

June 2017