BUDDLE FINDLAY

Legal update on information and communication technology - June 2014

Steve Nightingale, Philip Wood, Allan Yeoman, Amy Ryburn

3 June 2014

SaaS and escrow - Is it time to think harder about business continuity for SaaS solutions?

The software as a service (SaaS) market continues to grow as more customers shift from an on premise software licence model to cloud based solutions to address their business needs. However, for hosted SaaS offerings, a problem with the provider (such as insolvency) could leave a customer with no access to the software and, even worse, no access to the customer's data stored on the provider's system (or elsewhere). This article looks at the limitations of traditional escrow for SaaS solutions and identifies potential alternatives.

Traditional escrow

Traditional escrow is intended to ensure that the customer has continued access to the underlying software source code to enable it to support and maintain software that has been installed on its own systems. It generally involves the customer, the licensor and an independent third party (the escrow agent) entering into an agreement under which:

- The licensor deposits a copy of the source code (and often related documentation) for the licenced software with the escrow agent
- The escrow agent agrees that it will release that source code (and related documentation) to the customer if certain trigger events occur (such as the licensor's insolvency or material breach of the software licence or support agreements).

The key disadvantages of traditional escrow in relation to SaaS are:

- Given the object code for the software is not installed at the customer's premises and the customer has no relevant hardware platform, even if the licensor placed both the source code and object code in escrow, on release of that code to the customer it may take some time for the customer to actually procure the necessary hardware and build itself a working version of the system. Furthermore, given that the customer in a SaaS model never has a copy of any code in relation to the software or any information about the hardware environment on which it runs, it is perhaps even less likely that the customer will have the relevant technical expertise in its IT team to operate the system in-house even if it could get a copy of all relevant code.
- In a SaaS model the SaaS platform often holds the data rather than the customer. Insolvency can happen very quickly and once the liquidator, receiver or administrators have moved in, it may be difficult for the customer to obtain copies of its data or get the migration assistance it needs to put the data on any working version of the system it manages to put together. Additionally, if the SaaS provider uses a third party to host the software and data, this may further complicate the customer's attempts to recover its data given the customer will not generally be a party to the hosting agreement.

Of course, the customer could mitigate the 'data risk' to some degree by ensuring that it has the right to terminate the SaaS agreement if there are signs of material financial distress and by either backing up the data itself on a daily basis or by requiring the provider to provide the customer (or the escrow agent) with regular copies of the customer's data in a useable/compatible format so that the customer could put it together with the source code to replicate the system. Both of these options may have cost implications. In any event, they don't address the risk of the customer simply not being able to build (and get up to speed with running and maintaining) the replacement system quickly. This leaves the customer exposed to a business continuity risk where it may be left without a working system for a period of time.

What are the alternatives?

SaaS escrow

Some overseas escrow agents are now offering "SaaS escrow" solutions where the escrow agent keeps a mirrored standby of the system (including object code and data) which the customer can obtain access to if a defined trigger event occurs. The key advantage of this option is that it ensures immediate access for the customer to a working system and the customer's data, which

the customer may utilize until it is able to either recreate the technology in-house or source and implement an alternative system. However, SaaS escrow may well result in substantial additional costs to the customer.

For completeness, even if a customer has a "SaaS escrow" solution in place, it may also wish to have a traditional escrow arrangement in place for the source code, which the customer would be entitled to use for ongoing maintenance of the mirrored system.

Recovery services from hosting provider

It is not uncommon for SaaS providers to use third parties to host the SaaS provider's software and customers' data. For simplicity, given the software sits on the hosting provider's infrastructure, the customer may be able to obtain a recovery service / access to a mirrored system directly from the hosting provider. As with SaaS escrow, the parties would need to clearly specify the trigger events upon which the customer would obtain access to the recovery / mirrored system and data.

While such services do not appear to be readily available in New Zealand at this time, a customer could certainly ask for such an arrangement to be put in place either by entering into a three way agreement with the SaaS provider and the hosting service provider or by approaching the hosting provider directly.

This option may be lower cost to the customer than SaaS escrow, but the customer would be taking a risk on the ongoing solvency of the hosting provider.

Security interest with ability to appoint a receiver

The heaviest handed and most complex option available is for the customer to take a specific personal property security interest in the assets that comprise the functioning system (including software, data and related hosting contracts). The security agreement could give the customer the ability to appoint a receiver to take control of the system in priority to other creditors for a specified period of time. This would give the customer system/service continuity for a defined period while it transitioned to an in-house or alternative solution. Any secured creditors of the SaaS provider (eg its lending bank) would need to consent to the customer's security interest having priority over the other creditors' security interests.

While this approach is novel (and could be difficult and expensive to implement - especially if there are already existing security interests in place over the provider's assets), it provides an option that could be considered in circumstances where service continuity is critical and the customer has a lot of leverage in negotiations.

Conclusion

SaaS offers customers flexible solutions and low up-front costs, but until appropriate business continuity solutions are more readily available, those benefits are not without risks to the customer. We recommend customers engage with SaaS providers on these issues to ensure the risks are understood and minimised to the extent they can be. In particular, for critical business systems or data, we recommend that:

- Customers consider what the "plan B" is and how the customer can and will mitigate any data risks (as described above)
- Customers perform suitable due diligence on the SaaS provider (and monitor the provider's financial position on an ongoing basis) to assure themselves that the solvency risks associated with the provider are acceptable, given that it may simply not be possible from a legal and/or practical perspective to put in place arrangements that guarantee continued service continuity should the provider fail.

Fujitsu v IBM

Fujitsu Services Limited v IBM United Kingdom Limited [2014] EWHC 752 (TCC), the English High Court has recently considered preliminary issues in a contractual dispute. The case highlights the importance of careful drafting of exclusion clauses and is an example of how the courts will interpret technical, commercial agreements.

PwC was a party to an agreement for the provision of IT consultancy services to the Driver and Vehicle Licensing Agency. IBM acquired the PwC consultancy business. The provision of some of the services under the agreement was subcontracted to Fujitsu.

Fujitsu took action against IBM alleging that IBM had breached an obligation of good faith under the sub-contract and an alleged fiduciary duty IBM owed Fujitsu. Fujitsu's claims were principally based on allegations that IBM had failed to allocate work to Fujitsu in accordance with the contract. Fujitsu estimated it had lost £36.8 million in revenue.

As the contract contained limitation and exclusion of liability clauses, the interpretation of those clauses was critical to working out what (if anything) IBM could be liable for. The key preliminary issues were:

- Did the exclusion clause - "*Neither Party shall be liable to the other under this Sub-Contract for loss of profits, revenue, business, goodwill, indirect or consequential loss or damage...*" exclude all claims for loss of profits or revenue claims (even

where this would mean IBM would effectively suffer no financial detriment for its breach) or should it be restricted to exclude only claims for indirect loss of profit?

- Did the liability cap (of £5 million in any one Contract Year (as defined) and £10 million in aggregate) apply?
- Did IBM actually owe a duty of good faith or a fiduciary duty to Fujitsu?

The Court's approach to interpretation was fairly orthodox:

- The Court decided that any liability for damages for loss of profit/revenue was clearly excluded and that the liability cap applied. The sub-contract had been negotiated by sophisticated commercial parties at arm's-length. As the exclusion clause was reciprocal it could potentially benefit or disadvantage either party. In that context, the Court indicated that courts should be slow to intervene – particularly when the words of the contract were clear. The Court held that even though the clause excluded a remedy in damages, other remedies might be available to Fujitsu (eg declaratory relief, specific performance or a claim for account of profits by Fujitsu for wrongful gain by IBM).
- The Court also considered IBM's contractual obligation to have regard to "good industry practice" and the obligation on both parties to work together on an "open, honest, clear and reliable" basis. It determined that there was no express duty of good faith and it would not imply fiduciary duties in the arm's-length commercial relationship.

Virtualisation and software licensing

Understanding and complying with the terms of a software licence can be a complicated undertaking, and one which is not made easier by the widespread move by businesses and organisations from physical to virtual environments.

Virtualisation refers to the creation of a virtual version of a device or resource. This may be a server, storage device, network or even an operating system, where the framework divides the resource into one or more execution environments. Partitioning a server is an example of virtualisation because one server is partitioned to create two (or more) separate servers.

Many businesses have moved or are moving to virtualisation because of the substantially increased operational efficiencies and cost savings that result from its use. Virtualising software allows users to run multiple operating systems and multiple applications on one physical machine. This means businesses require less physical hardware, making it easier (and less expensive) to manage IT infrastructure. However, virtualisation also requires careful monitoring to ensure that software licensing compliance issues do not arise.

While some licences will allow for unrestricted use, or cater for virtualised environments, many software applications are still licensed on a traditional basis in which the number of users or installations is strictly limited to an agreed number. When software is assigned to a physical asset (eg, a PC or a server) on a one-to-one basis, it is relatively straightforward to count those physical assets in order to keep track of usage. However, if that software is deployed on a server that has been virtualised into two separate environments, then the actual number of installations could be two. If a licensee doesn't keep track of actual licence usage across a virtualised environment, then it may find itself exceeding usage restrictions in its licence. This non-compliance can generate significant penalties if the licensor decides to undertake an audit – something that is being seen more and more often.

This isn't helped by the fact that, if audited, licensees will generally be operating at a disadvantage – standard software licence agreements can be notoriously one-sided, and the licensor will no doubt have an information advantage over how the licence metrics apply (or don't apply) to virtualised environments.

When purchasing licenses from large software vendors there is usually limited, if any, scope to negotiate (or in some cases even discuss) the licence terms. Nevertheless, any organisation using virtualised environments (or considering a switch) should make sure they have a clear understanding of what their software licences allow.

Windows XP: Lesson for software upgrades and support

Attracting significant media attention, on 8 April 2014 Windows XP went out of support. This means that Microsoft will not provide any further security updates or technical support for XP. It has been estimated that there were still hundreds of millions of users of Windows XP when support ended.

This is a timely reminder to carefully review the provisions around upgrades of software and entitlement to support in software licences. It is not unusual for a software licence to state that the licensee must install all upgrades or that the licensor will only provide support for the software if upgrades are installed by the licensee. In addition, upgrades are sometimes at the licensee's cost or, even if they are not, the licensee will often be required to pay for any customisation required because of the upgrade.

While it is unlikely that a more favourable position would be able to be negotiated with Microsoft, it may be possible where the counterparty is a smaller supplier or where the software is not "off the shelf". That said, even the Microsofts of the world can find

themselves in hot water over decisions to cease support – earlier this month the Chinese government released new requirements for government tenders which included a requirement that Windows 8 be excluded from the bidding process on computer purchases. This was purportedly at least in part a response to Windows XP falling out of support.

Forget me not? The Google Spain judgment and the right to be forgotten

There may be millions of Europeans who this month will be quietly rejoicing the fact that those embarrassing high school episodes, drunken photos or other colourful aspects of their past may not be shaping their online identity for too much longer. The Court of Justice of the European Union (CJEU) in a recent judgment appears to have confirmed an individual's right to be forgotten on the internet. In doing so, the CJEU said that search engines have a responsibility to honour that right, in what comes close to a recognition that companies like Google essentially act as gatekeeper to the world's information.

The decision involved a request by a Spanish individual, Mario Costeja González, for Google Spain and Google Inc. to remove from its search results personal information contained in a 1998 newspaper article which Google had indexed. When Google denied the request, Mr Costeja González complained to the Spanish Data Protection Authority which ultimately referred the case to the CJEU.

The CJEU's decision was based on their conclusion that Google should be regarded as the 'data controller' of the information it indexes and displays in its search results – a term specific to European data privacy legislation, which refers to the entity that determines the purposes for which personal information is collected, and therefore has primary compliance responsibility. As the data controller, Google was responsible for ensuring that its processing of that information complied with the conditions set out in the European Data Protection Directive; in particular that the information remained relevant – in this case, the CJEU found that if information indexed and retrieved by a search engine appeared to be "inadequate, irrelevant or no longer relevant, or excessive" in relation to the purpose for which it was originally collected, then the information must be erased.

While the CJEU acknowledged that Google had an economic interest in processing the information, and other internet users had an interest in being able to access information, those interests had to be balanced against – and were, in this case, outweighed by – the individual's right to privacy under the Data Protection Directive.

The CJEU noted that this won't be the case in all instances – for example, where the individual is a public figure in whom there is a public interest. However, while the CJEU stopped short of expressly recognising a 'right to be forgotten', its decision and reasoning seems consistent with that concept (which itself has been the subject of much debate in privacy law reform around the world).

Of course simply wiping information from the internet is easier said than done, and one of the greatest practical challenges in protecting individuals from their past is how to overcome problems of multiple or remote publishers, or jurisdictional issues. More and more frequently the response to these practical difficulties has been to shoot the digital messenger, the search engine, by cutting off access to the information rather than dealing with the source of the information itself. New Zealand courts have hinted that, in the context of defamation, it is reasonably arguable that a search engine is a publisher of specific URLs and words, and that the defence of innocent dissemination might not be available once the search engine has been given notice of the defamatory material.

The CJEU's decision might be said to take this a step further, in putting the onus firmly on the search engines to take responsibility for ensuring that they store and index information on their servers in accordance with privacy laws.

Since the CJEU's decision (which Google's chairman has described as "flawed"), Google is said to have been inundated with take down requests to remove out-of-date information. Some commentators have voiced concern that search engines are likely to err on the side of caution and simply remove links rather than engage in an assessment of the merits of each individual case, and that the burden of regulating what information should and shouldn't be available via the internet will effectively be outsourced to a private company. Time will tell whether this is a role that search engines will play.

What do the Australian privacy law reforms mean for New Zealand businesses?

The recent reforms to Australian privacy law, and the introduction of 12 new Australian Privacy Principles (APPs), have been well documented. But what do they mean for New Zealand organisations doing business in Australia?

The Privacy Amendment (Enhancing Privacy Protection) Act 2012 came into force in Australia in March this year and introduced a new regime for entities that collect and hold personal information. The definition of 'personal information' has been expanded, required content of privacy policies is now prescribed, direct marketing is regulated more tightly, and organisations need to take more responsibility for overseas disclosures of personal information.

The enhanced obligations are backed up by the Australian Privacy Commissioner's stronger powers, including an ability to apply to the courts for civil penalties of up to A$1.7 million for serious or repeated breaches of the APPs.

For New Zealand businesses, the changes could be more relevant than they first think: the new requirements apply not only to Australian businesses, but to any entity with an 'Australian link'. An entity doesn't need to be incorporated in Australia, or even have a physical presence across the ditch, to have an 'Australian link' under the legislation – if an overseas entity collects personal information from people in Australia as part of carrying on business in Australia (eg, if products or services are marketed online to Australian customers), then they will be caught by Australia's privacy laws.

So what does this mean for New Zealand businesses with an 'Australian link'? For the most part, the APPs bring Australian and New Zealand privacy laws more closely into line – many of the APPs overlap with requirements that already exist in New Zealand's Privacy Act. In particular, businesses must ensure that their privacy policy sets out specific information on how the entity collects personal information, what it does with that information, whether it is likely to disclose information to overseas recipients, and how an individual can correct their personal information or make a complaint about an APP breach.

Most compliant New Zealand businesses will be doing this already, but the reformed Australian law contains requirements that go beyond the scope of current New Zealand privacy law – specifically, a tighter regime around overseas transfers of personal information, which requires entities to take reasonable steps to ensure that the entity receiving the information will not breach the APPs (with some exceptions). This will apply to transfers to group entities as well as offshore service providers, meaning that businesses will need an agreement with the overseas entity warranting compliance with the APPs.

Getting this right becomes important, as the disclosing entity can be held liable for a breach committed by the overseas recipient. Even New Zealand businesses without an 'Australian link' may find themselves on the end of a request for beefed up privacy provisions in their agreements with Australian affiliates, customers or suppliers, as Australian businesses look to ensure their compliance.

These changes are a good opportunity for businesses to take a look at their own privacy policies and methods of handling personal information, particularly where they have an 'Australian link'. In any case, many of the obligations imposed by the APPs could simply be identified as good practice, as well potentially indicating what any future New Zealand privacy law reform might look like.

Cloud computing - Public sector requirements

In October 2013 Cabinet agreed a cloud computing risk and assurance framework for government agencies. The framework directs that decisions on cloud computing be considered by agency CEOs on a case-by-case basis based on an appropriate balancing of risks and benefits. The Department of Internal Affairs (DIA) has now released the *Cloud Computing: Information Security and Privacy Considerations* document which outlines the security and privacy issues particular to cloud computing. Unless agencies are taking up all of government Common Capability cloud services, agencies are expected to use the processes in the document when considering the use of cloud computing services.

Amongst other things the document requires agencies to ask themselves a range of questions, including:

- How do the laws of countries where data is stored/processed affect the privacy of employees and/or clients?
- Is it appropriate to store the data in the relevant service in light of that assessment?
- How will data be used by the cloud computing provider?
- What dependencies are there on third party service providers? What risks do they pose?
- How secure is the cloud service digitally and physically?

The document outlines useful reference points on information security relevant to cloud services, including the Cloud Security Alliance's Security, Trust & Assurance Register.

The DIA cloud computing document is a very useful tool for both the public and private sectors on risks relating to cloud computing and is available here.

Auckland

188 Quay Street
Auckland 1010

PO Box 1433
Auckland 1140
New Zealand

P: +64 9 358 2555
F: +64 9 358 2055

Wellington

Aon Centre
1 Willis Street
Wellington 6011

PO Box 2694
Wellington 6140
New Zealand

P: +64 4 499 4242
F: +64 4 499 4141

Christchurch

83 Victoria Street
Christchurch 8013

PO Box 322
Christchurch 8140
New Zealand

P: +64 3 379 1747
F: +64 3 379 5659