BUDDLEFINDLAY

Legal update on technology, media and telecommunications - September 2016

Steve Nightingale, Philip Wood, Allan Yeoman, Amy Ryburn, Keri Johansson

27 September 2016

The Internet of Things - legal implications

The 'Internet of Things' is growing at an exponential pace as more and more devices are connected to networks. The market has been estimated to be worth US$11 trillion per annum by 2025. While there are plenty of opportunities for New Zealand business, there are a number of legal issues that will need to be carefully thought through – by both providers and users of the 'things'.

The key issues are likely to be privacy and security. Connected devices are designed to watch and to talk (to each other, to the device provider and also perhaps to a human user) and their value will often largely derive from the information they collect and share. While the collection of information by these devices may make the user's life easier or better, there are potential drawbacks. Firstly, users will have to be alert to how the information could be used and disclosed to avoid the information being used for purposes with which the user isn't comfortable (eg information about what's in your fridge being provided to your health insurer). Secondly, a security breach could cause a user significant problems (eg criminals accessing your credit card details through your fridge/toaster/bed, or your wearable technology that tells them nobody is home).

What the device provider is allowed to do with information collected can and should be addressed in the terms and conditions/privacy policies applying to the device. In basic terms, information collected should be used only for the purpose for which it was collected. This may seem obvious but in practice may be complex, particularly when:

- Many individuals interact with the same device (eg a fridge)
- Data from multiple devices is aggregated
- There are issues of consent to be worked through - who reads all the fine print on their smart phone, let alone when they plug in a new fridge?

Exclusive market control of the information collected by these observant devices may also give rise to competition law issues.

Security issues could also be addressed by regulation (including sanctions for security-related lapses) and/or by contractual requirements on providers (built into their terms) requiring them to maintain security to particular standards. But there is currently no significant specific regulation of the market. Furthermore, if you don't replace your fridge for 5 to 10 years, will the fridge software be kept up to date and secure from intrusions? It may well be difficult to apply updates and patches which may mean that users have to upgrade or replace devices or appliances more regularly than they might otherwise do to ensure that they stay secure. Will a TV manufacturer have to replace your TV if there is a security hack that can't be fixed remotely?

A good start might be common industry technical standards that limit the information collected and to whom it is passed, and that provide for the minimum security standards consumers can expect from certain types of connected devices. Some commentators have also suggested the use of data custodians – independent parties appointed to supervise the storage and management of data, and to control its access, release and use.

Finally, users and providers will both need to think carefully about what happens if the connected devices are broken or simply don't work as intended. If a device provides false information, it may still be relied on and very rarely questioned. Or a user may assume the connected device is looking after something and may not realise the device is broken until it's too late to avoid loss. It's not hard to think of scenarios where significant loss could arise – eg health devices that don't indicate a problem which requires a doctor's intervention or sensors used in agricultural processes that report faulty data leading to significant harm to crops. These sorts of liability issues are of course not new but the scenarios in which they might emerge will be. Most commercial customers will be used to thinking carefully about how loss might arise from use of a product and who should bear that loss. Consumers, on the other hand, may not be so accustomed to making these assessments – at least not when they are buying a home appliance.

This article was written by Amy Ryburn, partner in our TMT team, for the IITP Techblog (July 2016). The original article

can be found here.

Agile – Not just a line in a Statement of Work

Last month my colleague Andrew Matangi and I spoke at the ITx conference on contracting for agile projects. It was a great opportunity to meet a number of people who are involved in projects undertaken using an agile methodology. The conversations we had reinforced some of our concerns about how agile projects tend to be contracted for in New Zealand.

What we're finding in practice is that:

- 'Agile' means very different things to different people. It is a bit of a buzz word at the moment which means it is applied to very different projects – from iterative roll-outs of commercial off-the-shelf (COTS) products to development of innovative new software. Often before we can work out how to best contract for an agile project, the first question we have to ask is 'what do you mean by agile?'
- Agile methodologies remain really popular and anecdotally seem to work well for many projects. Many people we've met have used agile for a number of years and swear it leads to better outcomes. However, it's not uncommon to find that key people involved in ICT projects, including project managers, procurement specialists, and lawyers don't really understand the methodologies and so the contracts used aren't always fit for purpose.

'Agile contracts' in New Zealand still tend to take two forms:

- Use of a standard 'waterfall' master agreement with a statement of work or service schedule attached that says "this implementation will be conducted using agile". In some cases this can be a recipe for disaster because the 'front end' of the agreement simply won't reflect how the parties will work in practice. If this happens, the contract tends to be discarded pretty early on in the project (with the customer and supplier both acting as if it doesn't really exist) and, if the parties later end up in dispute, resolution can be very tricky
- Use of a supplier-friendly basic consultancy agreement where work is undertaken on a time and materials basis and there are few, if any, binding commitments to milestones and/or meeting specific requirements. This type of contract isn't always inappropriate but it is a difficult sell if the project is a high risk or costly with significant time or budget constraints.

In our view, just because a project is going to use an agile methodology, doesn't mean the parties need to abandon all standard contractual protections. We'd like to see more use of contracting models that are more sophisticated – contracts that reflect agile processes (eg sprints, early deployment of working software, product backlogs) and encourage innovation and learning as the project progresses but which also identify and fairly allocate project risks (eg inclusion of termination rights, pain/gain share fee models).

However, creating a contract that is appropriately tailored to the way in which a project will run and the parties' respective appetites for risk can take some time and unfortunately (depending on your perspective) requires the early engagement of your lawyers to ensure they are on board and don't just trot out a standard precedent.

This article was written by Amy Ryburn, partner in our TMT team, for the IITP Techblog (August 2016). The original article can be found here.

Help! We need a contract for our RFP

Over the past few years I've seen an increased public sector focus on producing better tender documents for ICT projects and designing procurement processes that are likely to lead to better results for government. However, it is still relatively common for standard ICT precedent agreements to be attached to the RFP at the last minute in order to meet the 'good practice' guidance in the Rules of Sourcing that proposed terms and conditions should be included in RFP documentation.

When a last minute call for a contract to attach to an RFP comes in, finding a precedent that is truly 'fit for purpose' can be extremely challenging. This is particularly true if the customer is open to a range of different solutions and implementation methodologies for the project (COTs vs bespoke, cloud vs locally hosted, waterfall implementations vs agile) that may require quite different contracts.

Attaching a 'standard' precedent can sometimes be risky:

- The contract may contain a number of 'red herrings' for potential respondents – eg equipment warranties and title clauses where there is no equipment being provided, detailed implementation processes that only reflect a waterfall approach, clauses that grant ownership of any new IP in the customer even if the solution is multi-tenanted. Red herrings can lead to confused (or confusing) proposals and could potentially put potential suppliers off responding at all

- Depending on how red the herrings are, there could be an impact on pricing if the respondent feels it is forced down a route that does not match how it operates its business. A generic template which gives an impression that the customer has a preference for a particular solution or approach (when it in fact doesn't), could also impact on how the respondents pitch their responses – potentially twisting their preferred approach to deliver what they believe the customer wants rather than playing to their strengths. Alternatively, some respondents simply choose to essentially ignore the contract – providing no or limited comments and hoping to negotiate better terms later
- The precedent, particularly if it has been around for a while, might not include detailed provisions about the things that may really matter to the customer (eg whether the supplier can use open source code in significant bespoke developments, how data back-ups are addressed).

There are of course a range of options to address the challenge. A few common options we see are:

- Early market engagement processes to work out what solutions might be available and help the customer to refine and identify what it is looking for before issuing an RFP
- Issuing a standard precedent (often in the form of a master agreement) but including instructions and commentary to respondents to give them guidance as to what parts of the precedent the customer anticipates may need to change and highlighting where the customer has some flexibility depending on the chosen solution
- Issuing high-level contract principles that set out the basic terms the customer would expect to apply regardless of the nature of the project and/or solution chosen.

The contract principles approach can be particularly beneficial if the customer anticipates that it may wish to select a supplier, such an offshore provider or public cloud provider, who may insist on using its own standard terms as a base. In such cases, it is often a good idea to also ask respondents to the RFP to provide any supplier terms that the respondent would propose (without any customer commitment to use them) and to require the respondent to explain in its response how any inconsistencies between the supplier terms and the customer's contract principles would be resolved. This can also help avoid the surprisingly common nasty surprise where the supplier late in the process (often once selected) provides additional 'mandatory' supplier terms (eg supplier or third party user licences that must be executed for the customer to receive the solution).

Whatever the approach taken, if the customer knows when it issues the RFP that the draft contract or contract principles may not quite fit the bill, it is important to leave sufficient time in the process for redrafting and negotiation. While it can be frustrating to select a supplier and then have to spend more time than you'd hoped tied up in contract drafting and negotiations, a robust contract reflecting the way the parties actually intend to work *and* the solution that is being provided is generally worth the time and effort.

This article was written by Amy Ryburn, partner in our TMT team, for the IITP Techblog (September 2016). The original article can be found here.

EU-US Privacy Shield, Brexit – Where to next for European Data Protection Law?

Arguments amongst UK and European politicians and privacy regulators could be dismissed as irrelevant to this end of the world. But Australian and New Zealand companies who operate in or are eyeing up Europe will need to keep up to speed with a number of recent changes to EU privacy laws.

For those who follow developments in European data protection law, the European Commission's vote to approve the EU-US Privacy Shield on 12 July 2016 may have been somewhat overshadowed by the result of the Brexit referendum just a few weeks earlier.

It had already been a big few months in the world of European privacy law. The General Data Protection Regulation (GDPR), the set of rules which will replace the EU Data Protection Directive, was agreed in December 2015 and will come into force in May 2018. The Court of Justice of the European Union declared in the *Schrems* decision in October 2015 that the Safe Harbour regime, under which US companies certified compliance with EU-standard data privacy practices, could no longer be trusted and was invalid.

The *Schrems* ruling caused a scramble among US companies whose businesses involve the storage or handling of European personal information to put in place alternative means of meeting EU data protection requirements. For Australian or New Zealand businesses with customers in the EU, inboxes would have been full with urgent requests from US hosting providers, SaaS vendors and other suppliers to sign up to 'Model Clauses' based on the European Commission-approved standard contractual terms for transfers from EU-based data controllers to offshore data processors.

Meanwhile behind the scenes, privacy and trade regulators from the EU and US were working hard to develop a more permanent solution. The result is the Privacy Shield, claimed to be a beefed up version of Safe Harbour with stronger

obligations on US signatory companies, clearer rights of redress and inquiry for EU citizens (including a dedicated ombudsperson), and assurances from the US government regarding access to data for law enforcement and national security purposes - an issue central to the *Schrems* decision.

The impact of Brexit

So, given the UK has voted to leave the EU, should we still care what happens to European privacy law over the next few years? Clearly, the answer is yes.

First, Brexit is only relevant, to any degree, to businesses whose European operations are headquartered in the UK, or who use data processing equipment located in the UK. For those with offices or equipment in other EU member states, European privacy law should go on largely uninterrupted, including with reforms as scheduled.

Second, it's unlikely that there will be any substantial change in UK data protection law in the foreseeable future. Brexit has a two-year runway so the English Data Protection Act 1998 and privacy directives from Brussels will remain the law of the land in the short-to-medium term.

Even in the long-term, post-Brexit it seems doubtful that the UK would choose a substantially different path from the rest of Europe. Significant commercial and trading hurdles could emerge if the European Commission found reason to declare UK privacy law 'inadequate', and compliance costs for UK businesses would dramatically increase. The more logical view is that the UK would, in the same way Switzerland has done, maintain a set of privacy laws that it knows to be consistent and harmonised with EU standards, minimising the disruption for UK businesses with customers and trading partners elsewhere in Europe.

However, the timeframe for Brexit means that UK businesses, and Australian and New Zealand companies who need to comply with UK data privacy law, will need to adopt practices compliant with the new GDPR when it is implemented in May 2018. So even as the UK is walking towards the exit, businesses will have to keep up with privacy law reform when the GDPR comes into force, and then re-adjust to whatever post-Brexit privacy regime replaces it.

The upshot is that it should largely be business as usual for Australian and New Zealand businesses in terms of the need for them to comply with European data protection laws. While the demise of Safe Harbour, its replacement with the Privacy Shield, the new GDPR and Brexit amount to a generation of reform and upheaval in the space of less than a year, it remains as important as ever for privacy compliance to remain near the top of the agenda for those operating in Europe.

This article was written by Allan Yeoman (partner) and Keri Johansson (senior associate) for the Australasian Lawyer magazine (Issue 3.4, August 2016).

The laws of New York? But I'm in Hamilton!

How many times have you signed up for services, especially online services and software, and discovered that any issues under the contract/licence/app terms are governed by the laws of some State of the USA, or some other jurisdiction thousands of miles from where you live? This doesn't just happen to consumers. Unless you are a major customer, many business contracts with overseas suppliers will require that the laws of some other country 'govern' the contract. What does this mean?

Let's say you sign up for Facebook. Facebook's terms state that all disputes under the terms of use (a contract) are governed by the laws of California, and, the parties have to bring any court action in California, and nowhere else. In practice this means if Facebook breaches the contract you have to sue them in California under a set of unfamiliar laws. These law and 'venue' requirements may make your complaint uneconomic to pursue in terms of both time and expense.

But that isn't the end of the story. Facebook is trading in New Zealand and, whether they like it or not, some New Zealand laws will apply to their activities, such as the Fair Trading Act or the Consumer Guarantees Act and its implied guarantees about the quality of consumer services. Also, if Facebook misuses one of your pictures, it might be infringing the New Zealand Copyright Act, giving you potential rights to sue for damages under that Act. In spite of this Facebook is quite cunning; their terms of use require that any court action between them and you can only be heard in California. This suggests that a claim under the New Zealand legislation might only be able to be heard in California, where it is certain they are unfamiliar with such claims.

Facebook is an overseas company; we can safely assume that most of their assets are in the USA (or maybe Ireland) and nothing significant lies within New Zealand. So, even if you can sue Facebook in New Zealand there may be no assets for your New Zealand High Court judgement to attach to. However, you may be able to take your New Zealand judgment and court orders to California and attempt to convince the California courts to enforce your New Zealand judgment there against Facebook's US assets. This will probably cost even more than the New Zealand proceedings but gives you some chance of recovering your losses.

Contracting with an overseas supplier, whether as a New Zealand business or consumer, in most cases leaves you in a pretty poor position if things go wrong if the governing law and venue are anything other than New Zealand. Even submitting to NSW or Victorian law in Australia may mean that in practice the cost of enforcing the contract with your Australian supplier is out of all proportion to the loss you have suffered. Does your MD have time in her calendar to go to Perth for a four day court hearing?

So what can you do? Try to get the governing law to be New Zealand law. Try to contract with someone with assets on the ground here in New Zealand. Finally, consider contracting with a big guy – if Microsoft messes up Excel or Word you won't be the only end user with a complaint, you will be one amongst a legion of aggrieved users.

Auckland

PwC Tower
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