BUDDLE FINDLAY

Legal update on TMT - December 2017

Allan Yeoman, Amy Ryburn, Philip Wood, Damien Steel-Baker, Keri Johansson, Renee Stiles

5 December 2017

A round up of recent legal developments that affect the technology, media and telecommunications (TMT) space.

Copyright law reform

It's been a decade since the Copyright Act 1994 (the Act) was last updated, and during this time, we have seen so much change - New Zealand's technology and media sectors have both blossomed and we are constantly finding new ways to consume, collect and exploit information. As a result, copyright is touching more and more New Zealand businesses. So when the Minister of Commerce and Consumer Affairs announced a review of the Act earlier this year, the announcement was widely welcomed.

The review is a great opportunity to make sure the law is up to date with new technologies, while still seeking to maintain balance between creators and users of copyright works, ensure the system works efficiently, and keep New Zealand in line with its international obligations.

The objectives of the review, as described in the terms of reference document, are to:

- Assess the performance of the Act against the objectives of New Zealand's copyright regime
- Identify barriers to achieving the objectives of New Zealand's copyright regime, and the level of impact that these barriers have
- Formulate a preferred approach to addressing these issues - including amendments to the Act, and the commissioning of further work on any other regulatory or non-regulatory options that are identified.

What is likely to be on the agenda?

The full scope of the review is yet to be announced, but we expect that two of the big issues discussed will be the possibility of introducing a broad 'fair use' defence, and a review of the current safe harbour provisions for Internet Service Providers (ISPs).

'Fair use' is a broad defence to copyright infringement that currently applies in the US and a handful of other jurisdictions. Supported by large-scale users of third party copyright works, a new 'fair use' system would arguably provide greater leniency and flexibility for the use of otherwise copyright protected works. Fair use is a truly technologically-neutral defence and does not need updating as we find new ways of exploiting existing copyright.

However, creators of copyright works are likely to argue that the US regime carries less certainty than the current exceptions-based approach adopted in New Zealand, the UK and most other common law countries. A question mark hangs over how well 'fair use' could work in a small non-litigious country like New Zealand (which has only had two fair dealing cases in the last 10 years), because it relies heavily on case law to help develop the boundaries of the defence and adapt it to new situations.

This question of a 'fair use' defence has already been broached across the Tasman by the Australian Productivity Commissioner. The Commissioner, with surprising finality, concluded that Australia's copyright laws "are skewed too far in favour of copyright owners…" and proposed introducing a 'fair use' exception from copyright infringement in Australia. However, the Australian Government has not directly supported the proposal, instead saying that the issue is complex and that it intends to "publicly consult on more flexible copyright exceptions" instead.

It is yet to be seen how seriously the 'fair-use' issue will be addressed back on home shores. If Australia's experience is anything to go by, it will be hotly debated on both sides.

The 'safe harbour' provisions in the Act provide ISPs (including online hosts and other intermediaries such as YouTube, Facebook and eBay) with safe harbours to limit their liability, where they are just an innocent conduit for infringing activities of third parties. MBIE's Creative Sector Study reported a growing level of frustration within the ICT sector of safe harbour regimes and the lack of effectiveness of current procedures for dealing with piracy, particularly internet streaming. Such frustration is not universal however, with proponents of internet freedom arguing that tighter controls are not the answer, and that problems with piracy are best dealt with by improving access to content.

Back when implementing the Trans-Pacific Partnership Agreement (TPPA) was initially on the cards, New Zealand was required to make a number of changes to the Act to meet its obligations under the TPPA. Interestingly, a number of those obligations are now off the cards given the recently agreed and newly-titled Comprehensive and Progressive Trans-Pacific Partnership, including the requirement to tighten laws around the circumvention of technological protection measures and the controversial extension of copyright protection to 70 years after the author's death. It will be interesting to see whether these changes are now dropped, or whether they are brought into force as part of the review - it may depend on the New Zealand Government's wider trade agenda.

What's next?

MBIE originally announced that it will release a broad issues paper for public consultation in early 2018, which will include a number of questions for public input. In the meantime, you can subscribe to MBIE's mailing list if you are interested in receiving updates on the review.

Blockchain update

Across the last several years, distributed ledger technology (DLT, or as it is more commonly referred to, 'Blockchain') has gone from the good idea underpinning Bitcoin to the tangible foundation of a potential technological revolution. For those still unfamiliar with the concept, we have written about it in the past.

As Blockchain technology has matured, mainstream commercial interest has well and truly been piqued. In 2017, the global business community have progressed from experimentation and proof of concepts to actual working prototypes for DLT systems, and even commercial application. The central concept of DLT - the ability to remove the current heavy reliance on a trusted intermediary to exchanges between transacting parties - is broad enough that significant investments are being made across a multitude of tech-related industries. This article will focus on several of the biggest publicised developments in Blockchain across the past six months.

State of the nation: Cambridge's inaugural global benchmarking study

This year saw the release of the world's first global benchmarking study on DLT. Undertaken by Cambridge University, the study gathered data from more than 200 established banks, DLT start-ups, and government institutions around the globe, and provides an empirical analysis of the use of DLT of both enterprise and public sector use of the technology.

The key takeaways from the Cambridge report are:

- To date, most DLT applications have been experimental, small-scale operations and have mostly been built as 'permissioned layers' onto public blockchains
- The majority of use cases focus on financial services, but there is also a significant amount of attention to non-monetary applications, such as identity verification and supply chain solutions
- The core infrastructure is being slowly improved, but shared protocols are still fairly undeveloped, meaning that interoperability of the different applications is still very limited
- Public sectors worldwide are among the most involved in DLT development, with 63% of central banks and 69% of other public sector institutions involved in proofs of concept
- Of those public sector institutions that are experimenting with DLT, 15% were planning to deploy applications in 2017, while a further 23 per cent plan to do so within the next two years.

The rise of initial coin offerings

This year has seen a remarkable growth in an alternative method of capital raising through Initial Coin Offerings (ICOs). ICOs are similar to the more traditional IPO (Initial Public Offering), but instead of issuing equity in the company to investors, the company running the ICO will issue a promise to build a particular blockchain-based product or service, and will give the investor digital tokens for that product.

According to research firm Smith + Crown, over $260m was raised through ICOs last year, with a further $560m being raised in the first half of 2017 alone. As popularity surges, many have seen a pressing need for ICOs to be more strictly regulated. At present, most ICOs are unregulated, and so are regarded as attracting investors with a 'high risk, high reward' appetite. In the US, the SEC is continuing to 'examine' options for consumer protection, while China has taken a stronger stance, outlawing ICOs.

New Zealand's regulatory body, the Financial Markets Authority (FMA), recently published its own commentary on ICOs and cryptocurrencies. The FMA's approach is for ICOs to be regulated on a case by case basis, as the specific characteristics of each ICO will dictate the ICO's financial product classification. The FMA encourages businesses considering ICOs to work collaboratively with the regulator to align their approach with the FMA's guidance.

Financial sector applications

It is undoubtedly the banking and financial services sector that is most closely connected with investment in blockchain applications. An IBM study in 2016 found that 91% of banks worldwide were then investing in DLT for deposit-taking. Many of these bank blockchains have since been commercialised and rolled out to the market.

Perhaps one of the most exciting applications for financial services is in respect of cross-border payments. This is an area with a lot of room for improvement, as the incumbent foreign exchange systems are slow, bureaucratic, and expensive. Remittance payments often go through multiple intermediaries through the course of an end-to-end money transfer. DLT has the potential to fast-track the process by cutting out the middle man.

The solution, or at least one of many forthcoming solutions, is now in market. In November 2017, global tech giant IBM launched what it bills as the first blockchain network for cross-border currency payments. The network was built in collaboration with stellar.org, a non-profit that creates low-cost financial services in a bid to fight global poverty, and KlickEx, a New Zealand money remittance operator. The product allows customers to verify the exact time that payments are sent, when the foreign exchange transaction occurred, and when the money was received. There is no longer the need to trust multiple intermediaries at either end of the transfer.

The benefits of such technology becoming accessible and affordable are immense, especially for developing nations. The question now becomes whether the likes of Western Union and big banks will follow KlickEx in adopting IBM's blockchain payment network. Tribalism has often been identified as an inhibitor to any one network gaining market ubiquity, and with the likes of Amazon and other non-traditional financial services players looking to compete with networks of their own, it remains to be seen whether the IBM cross-border blockchain can be a market-wide solution for cross-border payments.

Non-financial applications

There are also several non-financial applications that are looking to exploit the opportunities presented by DLT. One such area is personal data protection and control - and it's a timely development.

In addition to central government identity systems, there are many global firms that store huge quantities of our personal data and turn considerable profit from it, without any of the benefit necessarily coming to consumers. When those firms lose personal data (as Equifax did earlier this year, with data of more than 140 million people being compromised), there is often no recourse to the consumers who supplied the data.

DLT offers fresh opportunity for the control of this data to remain with individuals, by removing the need for a central third party to store and communicate the information between entities.

A development from the past couple of years that serves as a good example is the Estonian 'ID-Kaarts' system. The system uses shared databases to allow multiple parties to share authoritative information such as data-logging for clinical assessments or commercial deals. The result has been a secure, all-digital government experience, which has significantly reduced bureaucracy. Such systems can even allow individuals to easily access and create certified copies of any of their personal records, protected from anyone other than themselves by key-locked encryption. The ledgers themselves are also becoming more sophisticated, allowing for developments such as the ability to send documentation to others that need to see it, without compromising any of the control of access. This may also allow individuals to take back the value in their own data, and to choose whether they want to 'sell' their own personal information to businesses in the future.

While most of us have yet to directly benefit from the exciting possibilities that DLT holds, the past 12 months have seen DLT transform from potential disruptor to the foundation of truly marketable products. With more and more entities graduating their blockchain prototypes into actual service, the next 12 months promise to be a gruelling test of DLT, and whether it can silence its critics by making the difficult leap from 'good idea' to 'killer app'.

A tale of two suppliers

In the work we do for customers procuring ICT to meet their business and operational objectives, it seems like an increasing number of tender responses are joint responses where a local New Zealand entity is implementing an offshore software solution (often cloud-based).

On their face, these proposals can look very attractive. The customer gets the benefit of a potentially world-class technology solution at an attractive price, implemented by a company 'on the ground' which is more likely to be familiar with the New Zealand environment and may be more responsive to the customer's needs if it has a local reputation to protect.

However, from a customer's perspective, the two suppliers typically have no intention of entering into one tripartite contract where both suppliers are 'jointly and severally' liable for the outcome. Nor do they typically propose a contractual arrangement where one of those suppliers is responsible for licensing, support and implementation of the solution but subcontracts a portion of the required work to the other supplier. What they will insist upon instead is a structure where the customer signs up to a separate implementation contract with the implementer and licensing/subscription (and possibly support and maintenance) agreement with the off-shore vendor.

This contractual structure is relatively common and often may be the best (if not merely the only) way forward. However, there are several potential pitfalls to avoid. In our experience, they include:

Compliance with the 'requirements'

While global suppliers and local implementers may have put forward joint proposals, we quite often see them squabbling over who will be responsible for ensuring that the solution meets the customer's RFP requirements - sometimes with an outcome that the customer is left carrying the risk. An implementer may be reluctant to warrant, for example, that the solution once configured and implemented will meet the customer's functional and/or non-functional requirements if it has not developed the solution itself. The offshore vendor may only be prepared to warrant that the solution meets its published specifications. Getting either party to commit that the solution, once implemented, will meet the customer's requirements, can be very challenging. In our experience, this needs to be called out as an express expectation in the RFP to have the best chance of successful resolution.

We recommend that customers make it very clear from the outset in RFP documentation that (a) the customer is not the expert in the solution and is relying on the response to the RFP and (b) the customer requires that the successful respondent(s) commits in some way to meeting the customer's requirements. If push back occurs during negotiations, we often find that the best approach is to insist that the two suppliers together resolve the issue and put forward a joint response that addresses the concern before either will progress in the RFP process.

The impact of failed implementation on licensing

We often see global suppliers insisting that the customer order a certain number of subscriptions or licences before development and testing even commences. The obvious problem with this is that the customer does not, at the outset, have a configured and accepted solution and is dependent on another party (the implementer) doing its job to achieve this. We typically seek to negotiate a position that if the implementation fails (ie acceptance of the solution is not achieved or is delayed so long the customer ends up terminating) either (a) the global licensor/provider must refund the licence fees paid up until that point or (b) the implementer must pay the customer an amount equal to those licence fees.

Liability

If separate contracts govern implementation and subscription/licensing, you'll typically find that both suppliers want to tie their respective liability cap to a multiple of the fees they have been paid. The problem with this is that the implementation fees might be relatively small but this might be the stage at which the customer faces the biggest risk and potential losses. Without a cap that is tied to the amounts paid to both suppliers, the cap in either or both contracts may be too low and may require some careful consideration and negotiation. Furthermore, an ability to recover up to a cap is only valuable if the party on the hook has the financial standing to meet the potential liability (or is appropriately insured). For example, even if a local implementer agrees to a high cap, that won't help if (a) the offshore supplier won't guarantee the implementer's performance; and (b) the local implementer is a small company with limited assets or insurance.

To ensure customers enter into these contractual structures with 'eyes wide open', we suggest that RFP processes require joint proposers to clearly explain their position on risk allocation. This should include requiring them confirm whether they intend to have joint and several liability for the solution as a whole (and all related services). If the answer to that question is no (as is often the case), they should specify what each joint respondent intends to be liable for and to what extent, provide separate financial information about each proposed contracting entity, and propose any other means by which risk to the customer might be addressed (eg guarantees, performance bonds).

Support - whose job is it?

Time and time again we see support becoming a very fraught area of negotiations, particularly if it isn't given much attention until the close of the deal. Support can account for a small proportion of the overall fees and therefore viewed by the customer as a comparatively easy issue to close out. However, despite the lack of money at stake, support can be crucial in terms of the ongoing viability of the system. Having less financial incentive to drive a support partner to find a suitable outcome, if this isn't dealt with early on, customers can find themselves close to the end of the deal before they find out that they won’t be able to receive a key element of support that may leave them exposed.

A local implementer will typically make the most margin on implementation services and have not much interest in providing local support (or, even if it does, may not wish to commit to binding service levels). An offshore provider may have a very limited support offering (sometimes limited to time zones that don't work for NZ clients) and little appetite for changing the offering (particularly if they are offering a one-to-many, subscription-based service). Customers can therefore struggle to get the support they need and so the benefit of having a local implementer on the ground needs to be balanced against the ongoing BAU requirements of the customer.

Our advice - even if the support seems likely a relatively small portion of the deal (at least from a financial perspective), focus on support requirements early in negotiations to avoid a situation where you are presented with a support offer and terms at the last minute which you have little choice but to accept.

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