BUDDLE FINDLAY

Legal update on TMT - November 2018

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

15 November 2018

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

The Office of the Privacy Commissioner moves to Azure

The Office of the Privacy Commissioner (the OPC) is moving to Microsoft Office 365 and Azure cloud services (delivered from Australia) and has released its privacy impact assessment (PIA) of these services. The PIA sets out the OPC's assessment of the key privacy risks and how the OPC was satisfied that it could mitigate those risks (including a comparison with the risk of continuing to use an on-premise solution).

As the regulator of the Privacy Act 1993 and the use of personal information in New Zealand, the OPC would know its use of cloud services would be under scrutiny. Its PIA has been proactively published and is written with public consumption in mind. It is a great example of a well written and easily digestible assessment of the privacy concerns with using offshore cloud services, and is recommended reading for anyone doing a PIA for a major cloud service, whether Microsoft or any other provider.

Some of the areas the PIA addresses include:

- The application of Australian law
- The risk of overseas government or law enforcement agencies accessing data
- Contractual and legal controls to ensure control of data is retained
- The steps the OPC is taking to ensure its customers are informed about where their personal information will be stored.

The full PIA is available here.

Extra territorial reach of the GDPR tested

The United Kingdom's Information Commissioner's Office (ICO) has issued the first formal enforcement notice under the European Union's General Data Protection Regulation (GDPR). The enforcement notice has been issued against AggregateIQ Data Services Limited (AggregateIQ), a data analytics provider based in Canada. This is the first action taken by the ICO outside of the United Kingdom.

GDPR terms

In summary, the GDPR applies to companies and individuals outside of the European Union if they:

- Have a presence in the European Union (eg an office or a branch)
- Process the personal data of individuals within the European Union in connection with the offering of goods or services
- Monitor the behaviour of individuals within the European Union.

ICO findings

As part of an ongoing investigation into the use of data analytics in political campaigns, the ICO has found that AggregateIQ used personal data provided to it by a number of political organisations to target online advertisements to voters in the United Kingdom. The advertisements related to the United Kingdom's referendum on membership of the European Union and were largely created on behalf of Vote Leave.

The ICO concluded that AggregateIQ breached the GDPR by using personal data in a way that data subjects were not aware of, for purposes they would not have expected and without a lawful basis for that processing. In addition, the processing was incompatible with the purpose for which it was originally collected and the relevant data subjects were not informed of the

necessary details of that processing.

If AggregateIQ fails to comply with the enforcement notice, the ICO may serve a penalty requiring payment of up to 20m Euros, or of 4% of an undertaking's total annual worldwide turnover, whichever is higher. As the first extra-territorial enforcement notice issued under the GDPR, much attention will be paid to the level of the fine sought by the ICO.

AggregateIQ is currently appealing the ICO's findings.

Extra territorial impact in New Zealand

AggregateIQ's enforcement notice is an important reminder for New Zealand companies that they may be subject to the terms of the GDPR (even where they are not established in the European Union). However, as AggregateIQ's processing of voter personal data was particularly politically sensitive, it remains unclear how the GDPR's extra territorial provisions will be applied and enforced in respect of more mundane data processing. For the time being, we consider that in most cases a pragmatic and proportionate approach should be taken to the application of the GDPR until further clarity and guidance is available.

Can GDPR and blockchain get along?

Blockchain technologies are increasingly being promoted as a potential solution to a variety of data processing operations, largely due to blockchain's features of immutability, anonymity and decentralised control. For those still unfamiliar with the concept, we have written about it in the past.

However, for those businesses who are currently or are considering utilising blockchain technologies, consideration may need to be given to the consistency between blockchain and applicable privacy law. In particular, several of the requirements imposed by the GDPR (eg the right to data erasure, the right to correction of incorrect data and the right to restrict processing) appear to be difficult to reconcile with the operation of blockchain networks. While New Zealand privacy law does not go as far as the GDPR, some of the privacy principles enshrined in the Privacy Act 1993, such as Principle 7 (correction of personal information) and Principle 9 (not holding personal information for longer than necessary) are arguably equally problematic for organisations looking to utilise blockchain technology.

Recently, France's data protection authority (the CNIL), has published a report on blockchain and the GDPR. The CNIL report proposes several options to minimise the privacy risks that arise from the use of blockchain technologies, including storing the majority of the relevant data outside of the blockchain (or 'off chain') to mitigate data retention and erasure issues.

This seems to be a common approach which is being explored around the world. However, CNIL acknowledges that the solutions proposed require further consideration and innovation to ensure that they are workable in practice. CNIL also emphasises that blockchain technologies should not be implemented unless businesses are able to establish that blockchain is the most appropriate technology for the processing of personal data.

Next steps

CNIL considers that the matter needs a harmonised European approach to ensure that there is a robust approach to privacy law and blockchain. The European Parliament has echoed this sentiment in its recent resolution regarding distributed technologies and blockchains, calling on the European Commission and data protection supervisors to provide further guidance on the matter. In the meantime, blockchain continues to promise a technological revolution, but its ability to deliver on that promise in practice remains largely untested.

What’s the point of a warranty period in a SaaS contract?

We are increasingly seeing significant gaps between suppliers and customers of SaaS contracts in relation to their expectations about the purpose and effect of contractual warranty periods.

The use of warranties and warranty periods in on-premise software licences is long-standing. Typically, a supplier would offer a period after delivery (or, if the customer was able to negotiate this, acceptance of installed software) during which if the software contained major bugs or failed to meet its specifications, the supplier was in breach of the warranty and had to fix the problem – usually entirely for free. Negotiations often centred on the issue of whether, assuming the defect/non-compliance was fixed, the supplier had any liability for losses that might be incurred in the meantime – with many suppliers insisting that the fix was the customer’s sole remedy.

Warranties in relation to tangible goods have obviously been around for a long time and a short warranty period often makes a lot of sense. You might expect a product that you buy in a shop to work as promised for a relatively short period of time before normal wear and tear impacts on its operation. But these historical justifications for warranty periods arguably makes less sense for software – while software wear and tear/'software rot' may indeed occur, it tends not to happen over a short period of time.

Rather, the key objective/purpose of a warranty period in a traditional software licence could alternatively be viewed as essentially giving the customer a benefit of a period of free support/maintenance to fix any errors – in turn incentivising the supplier to make very sure, at the point of delivery or acceptance, that the software is correctly installed and in good working order.

This benefit can fast be eroded in the terms of SaaS/cloud contracts. This is because the support/maintenance services and fees are often wrapped into the subscription service and are payable from day 1 – there is no period of free support or maintenance – and supplier standard SaaS terms often provide that fixing the warranty breach is the customer's sole remedy for the breach.

From the customer's perspective, this approach doesn't offer any additional benefit for a period after delivery/acceptance – in fact the warranty period sometimes presents more risk to the customer than the ongoing subscription term once the warranty period has expired. This is because:

- The customer may be already paying for support/maintenance in the form of a bundled subscription fee. In such circumstances, it can be unclear whether the customer is actually getting for free (as opposed, for example, to a situation where support and maintenance is charged for on a time and materials basis but time spent on warranty fixes may not be charged)
- If the warranty fix is expressed to be the sole remedy, then the customer can't recover additional losses in the form of damages (should it wish to do so) – although of course in practice additional losses may be difficult to prove and recover
- Often the supplier will argue that the service levels don't apply during the warranty period but rather the supplier has a 'reasonable' period to fix defects in breach of warranty. The customer can therefore end up with less certainty about when a fix must be provided than when it is in the BAU support phase after the warranty period has ended.

We've been involved in projects where:

- The customer expects the solution to be near perfect at go-live so that if there are any problems in the warranty period, the supplier should bear the full risk of these (both the cost of fixing them and any losses the customer suffers as a result) and should meet all the service levels as it does so
- The supplier expects there to be bugs and problems in the period after go-live that need to be ironed out and, so long as they act to fix these in a professional manner within a reasonable timeframe from discovery, doesn't expect to have any further liability.

Clearly these are quite different philosophies. What is a reasonable position to take will often depend on the nature of the solution, the level and structure of the fees payable, the parties' appetite for risk, and the development methodology.

In our view, there isn't actually any right or wrong answer to the question posed in this article. The 'point' of a warranty period depends very much on what the parties negotiate it to be and how any warranty terms interact with the other clauses of the contract (eg termination rights and general performance obligations) and rights and remedies which exist at law (eg the right to damages).

What is important is that contracting parties realise that warranties in IT contracts don't necessarily have any 'magical' qualities - the benefits of warranty periods may be largely illusory. It is important to:

- Understand at the outset what you are seeking to achieve by having a warranty period
- Identify whether the parties are actually on the same page about this
- Ensure that the contractual provisions (including the interaction with other rights and remedies) actually achieve the agreed objective.

Can I interest you in a firewall for your toaster?

In September, the California state legislature enacted two identical bills regulating Internet-connected devices sold in California, aimed at developing minimum security standards for devices that make up the 'Internet of Things', or 'IoT'. The bills are among the first regulatory measures to be implemented worldwide that are specifically aimed at hastening the industry's response to the threat of IoT-based cyber-attacks.

The IoT is the name given to networks of devices that have components that allow them to connect to the internet, and that communicate with each other via this internet connection. IoT networks allow businesses and consumers to automate the completion and co-ordination of tasks (including making transactions) via the interconnected devices to make businesses more efficient, and domestic life easier. IoT-connected devices have been widely available on the consumer market for several years, and further commercial applications for the IoT concept are continuing to be developed. Recent reporting indicates that the value of transactions conducted through the IoT will experience a compound growth rate of 13.6% over the next five years, meaning that some $1.2t US may be transacted via IoT devices annually by 2022.

With the popularity of IoT-enabled devices (and with it, the amount of money being funnelled through IoT transactions) rapidly growing, the need for protecting users through effective regulation has already become apparent. A recent report by research

firm Gartner found that nearly 20 percent of organisations that had deployed IoT-capable devices had experienced at least one IoT-based cyber-attack in the past three years. In January 2015, the US Federal Trade Commission (FTC) released a report that outlined the inherent privacy and security risks associated with mainstream IoT adoption, and urged manufacturers to (among other measures) build security hardware into IoT devices from the outset to insulate against third party attacks.

At the time that the FTC issued its report, it seemed that it would be in the best interest of IoT stakeholders to adopt the recommended 'best practices' when it came to security protocols in IoT products, even without a regulatory mandate. After all, it was essential that consumer confidence could be maintained in order for mainstream consumers to embrace IoT technology, and even one major security compromise could have a stifling effect on the burgeoning industry. However, for economic reasons, this has not been the unanimous response from manufacturers. For many manufacturers, consumer demand for IoT devices is not yet at the level so as to enable significant investment in security features. As a result, there are still many devices on the global market with little to no built-in security, which could have the potential to compromise the whole of any network that such devices are connected to.

The California legislation is drafted broadly, both in the scope of its application and in its requirements for compliance. The regulations will apply to any devices that are manufactured in California and are "capable of connecting to the internet, directly or indirectly", and require manufacturers to equip all captured devices with "reasonable security features that are appropriate to the nature and function of the device … [and] the information it may collect, contain or transmit… [to protect] from unauthorised access, destruction use, modification, or disclosure". While on one hand the non-specificity of the requirements for compliance allows for manufacturers to flexibly apply their own interpretation of what is 'reasonable', some manufacturers have called the wording 'egregiously vague', and have criticised the advantage that it gives to parallel importers of goods manufactured elsewhere, that are not subject to the same restrictions.

The latter point may become less of an issue in coming years, as it is expected that other jurisdictions will follow in California's footsteps. Though falling short of placing obligations on manufacturers, a federal bill is currently before the US Senate that would require US state departments to have certain clauses relating to security in any contract for the procurement of IoT devices, which would theoretically give manufacturers a commercial incentive to adopt robust security protocols. In the European Union, some IoT devices fall under the jurisdiction of the General Data Protection Regulation (GDPR) due to their data sharing and processing function. This means that not only are IoT device manufacturers compelled to consider security due to the GDPR's 'privacy by design and default' requirements, but also that IoT manufacturers or operators may need to provide facilities that allow users to communicate their consent to certain data being shared. The application of the latter requirement may be difficult to pinpoint, given the connected and automated nature of the IoT. The EU also has in place a general directive aimed at cyber security which may impact IoT. The Directive on security of network and information systems (NIS Directive) does not place specific obligations on IoT device manufacturers, but does create a framework at the European community level for cyber-security notification processes, which may allow EU member states to more easily implement and enforce mandatory security requirements such as those now in place in California.

In New Zealand, the regulatory response has been slower to materialise. At present, an association of industry stakeholders (the New Zealand IoT Alliance) is administering a series of working groups that are aimed at developing industry standards and guidelines for a number of facets of IoT, including cyber security, data/privacy, and device certification. In the meantime, the New Zealand Cyber Security Strategy published in December 2015 (NZCSS) essentially promotes a 'buyer-beware', reactive approach to security of internet-connected devices, including IoT devices. The NZCSS also established the Computer Emergency Response Team (CERT), which serves as an industry watchdog, issuing public warnings of cybersecurity threats, and working with businesses and organisations that are affected by cyber attacks.

As is common with emerging technologies, the regulatory response to IoT security has struggled to keep pace with the development and adoption of the technology itself. In some places (including New Zealand), we are seeing this widening gap being filled by self-regulation from industry stakeholders, while other places serve as examples of the struggle to reconcile 'industry best practice' with harsh market realities. The new California legislation, through its deliberate vagueness, arguably serves as an indicator that regulatory development of the IoT space will continue to be industry-led for the time being, until a clearer picture of the risks and dangers can emerge. In the meantime, it seems likely that lawmakers around the globe will continue to monitor the early legislative efforts of places like California - while using their available tools to promote the development of their domestic IoT industries without putting consumers at undue risk.

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