BUDDLE FINDLAY

Legal update on TMT - June 2017

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

1 June 2017

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

Another win for the computers - predictive coding discovery endorsed in Australian court

Late last year, the Supreme Court of Victoria released a judgment that resolutely approved the use of predictive coding (or TAR - technology assisted review) for the purpose of discovery in a large litigation matter, the first decision of its kind in Australia.

In *McConnell Dowell Constructors (Aust) Pty Ltd v Santam Ltd & Ors (No 1)* [2016] VSC 734, the lawyers involved in the dispute faced 1.4 million potentially relevant documents for review, a number already reduced down from a massive 4 million documents using de-duplication software. The Court estimated it would take a solicitor 583 working weeks to get through them. The parties were unable to agree on a solution between them, so turned to the Court for guidance.

After engaging a special referee to assist in answering questions on discovery processes, the Court and the parties agreed to use predictive coding and the Court made an order to that effect.

This is the latest in a series of cases across multiple jurisdictions that recognise and give momentum to this emerging technology. Commentators expect to see an increased use of the technology in Australia now that a court has formally approved it.

So what exactly is predictive coding, is it reliable, and have the New Zealand courts sanctioned its use?

Predictive coding is a sophisticated software that performs the task of reviewing documents for relevancy in a proceeding. Document review is usually carried out by solicitors working on the matter who have an understanding of what may or may not be relevant. As large commercial disputes can involve millions of documents, the discovery phase is incredibly costly and can drag out the litigation process considerably.

Predictive coding greatly reduces the time and costs involved in discovery, as much of the work is done by a computer. The process includes measures that ensure the software performs the task as accurately (and as much like a human) as possible.

The predictive coding process was summarised in the UK decision *Pyrrho Investments Limited v MWB Property Limited* [2016] EWHC 256 as follows:

- The parties settle on a predictive coding protocol that outlines how the software will do its job
- A solicitor who would otherwise be carrying out the review would then take a sample set of documents, decides on their relevancy and categorises them appropriately
- The software is then 'trained' using this sample batch of documents to complete the same job for all the documents. The software analyses the documents for common concepts and language used
- The software then carries out further quality assurance exercises before a sample is selected for review by the solicitor. Where the solicitor overturns decisions made by the software, this decision is fed back into the system for further learning
- The process of overturning may be repeated several times until a suitable level of agreement is reached
- At this stage, a list of relevant documents can be produced.

Evidence suggests that predictive coding is at least as accurate as, and probably more accurate than, the manual method of identifying documents (examined in *Irish Bank Resolution Corporation Ltd v Quinn* [2015] IEHC 175). The key is to be consistent during the human-assisted stages, and to agree carefully on parameters beforehand.

New Zealand Courts are yet to examine predictive coding and, perhaps for this reason, the technology is not utilised extensively in discovery here at this stage. However, as far back as 2011, our High Court Rules (HCR) have referred to predictive coding or 'document prioritisation technology' as an option for discovery, and state that parties should consider and agree on whether such

methods are appropriate in the case at hand. Judge David Harvey has spoken about the benefits of predictive coding, via obiter remarks in *Dotcom v United States of America* [2012] DCR 661 and in articles published on the Auckland District Law Society website. In *Dotcom,* Judge Harvey reminded the parties that "there are procedures available…in the civil arena that will enable the prompt disclosure of relevant information", including predictive coding.

So while predictive coding remains in its early stages and has not been carefully examined in our courts, there is acknowledgement of the technology within New Zealand, and several well-regarded judgments from other jurisdictions that would be persuasive if the question arose here. It's worth remembering that a court sanction is not actually needed. Parties can agree between themselves to use predictive coding but, as the decisions in other jurisdictions indicate, parties seem inclined to first seek guidance from the court.

Under the High Court Rules parties are obliged to co-operate to ensure that the processes of discovery are proportionate, to consider options to reduce the scope and burden of discovery, and to ensure technology is used efficiently and effectively. Predictive coding will no doubt take hold as an effective tool to make information manageable in litigation in this increasingly digitised world.

What's in a name? - Enforcement powers and the Naming Policy under New Zealand's Privacy Act

New Zealand's Privacy Act provides a number of enforcement options to deal with information privacy breaches by organisations holding and using personal information (referred to in the Act as 'agencies'). Those powers have not, however, changed significantly since the Act first received royal assent on 17 May 1993. In the meantime, the internet, social media platforms, smartphones, big data and vast customer databases have been behind an astronomical increase in the scale and sensitivity of personal information collected and used. With that same technology, of course, comes an increased risk of misuse and likelihood of harm.

While reform has been on the New Zealand legislative agenda for some time, the recently introduced 'Naming Policy' provides New Zealand's Privacy Commissioner with a useful (if interim) stick with which to wave at transgressors of the Act's Privacy Principles.

Status quo - the Act, the role of the Privacy Commissioner and the Human Rights Review Tribunal

The Privacy Act was enacted to promote and protect individual privacy, establish principles with respect to the collection, use and disclosure of personal information, and appoint the Privacy Commissioner.

However, the Commissioner's role is not, and has never been, focused on enforcement. The Office of the Privacy Commissioner is instead charged with promoting education about privacy principles, monitoring legislation, and issuing codes of practice specific to particular types of information or information processing.

The Commissioner also acts as a mediator of sorts, receiving and hearing complaints from those that feel that their privacy has been interfered with in some way. The Commissioner may also commence an investigation on their own initiative (known as an 'own motion investigation'). When presented with a complaint, the Commissioner will investigate the situation and act as a conciliator between the individual(s) concerned and the agency alleged to have breached the Act. The majority of complaints made to the Privacy Commissioner are resolved or settled in this way.

However, the Commissioner has no statutory powers to award a complainant compensation for breaches of the Act, or to order apologies or changes in practice. For complaints to be taken any further, they need to be referred or appealed to the Human Rights Review Tribunal, a specialist forum established under the Human Rights Act 1993 (the Tribunal). There are two routes that a privacy-related complaint can take to reach the Tribunal: the Commissioner may refer the matter to the Tribunal, or the complainant can take the matter there directly. The decision of the Tribunal on a Privacy Act complaint is legally binding, and the Tribunal is able to award a variety of remedies. These remedies include:

- Declaring that the action of the defendant is an interference with the privacy of an individual
- Awarding damages of up to NZ$200,000
- Issuing an order that restrains the defendant from continuing or repeating the interference with privacy.

The Tribunal's highest award to date was for NZ$168,000 in 2015. The case (which became known as the 'Facebook Cake Case', *Hammond v Credit Union Baywide* [2015] NZHRRT 6) arose from an employment dispute in which the complainant shared privately to friends over Facebook photos of a cake that she had decorated with obscenities referencing the complainant's former employer. Having heard about the cake, a senior manager of the employer pressured one of the complainant's friends (and former colleagues) to show them the photo, and then circulated the image widely amongst the company, its senior staff and recruitment agencies in the region together with a warning that the complainant should not be hired.

The Tribunal determined that the employer's conduct was a breach of one of the more fundamental privacy principles in the Act, preventing disclosure of information for purposes other than for which it was originally collected. The Tribunal awarded damages

as compensation for humiliation, loss of dignity, injury to feelings and loss of income. Prior to the Facebook Cake Case, the highest award had been NZ$40,000 in the 2003 case *Hamilton v The Deanery 2000 Limited* (29 August 2003) HRRT 36/02, Decision No 28/03, where a treatment clinic disclosed sensitive personal information to immigration officials. The shift in quantum of damages indicates in part an increased concern with the potential seriousness of breaches in the current digital climate.

The introduction of the Naming Policy

In December 2014, the Naming Policy came into effect. Introduced by the Commissioner, the Naming Policy outlines the Commissioner's practice of naming organisations that have been found to have breached the information privacy principles in the Act.

In developing the policy, the Privacy Commissioner stated, "We think it is time to 'name names' where it is warranted. Our view is that in certain circumstances, the Privacy Act is better served by revealing the organisations that have breached the law." Naming can occur in a number of ways, including through the publication of the Commissioner's case notes and associated media releases, annual reporting, formal reports to Ministers or Parliamentary committees, and publication of open letters calling upon organisations named in media reports to explain their actions.

The Naming Policy does not mean that all organisations that breach the privacy principles will automatically be named. Rather, the policy sets out the factors that the Commissioner will take into account in deciding whether to name an organisation. Those factors include the seriousness of the breach, the number of people affected, whether there have been repeated breaches, and whether the organisation has demonstrated an unwillingness to comply with the law. A key consideration will also be whether, in the circumstances, the public interest would benefit from identification of the organisation, due to its deterrent effect, educative purpose, or other reasons.

The road to reform

Resorting to naming non-compliant organisations has been seen by some as a sign of the Commissioner's frustration at the lack of effectiveness of the Act's current enforcement framework, and the Government's delays in introducing a new Privacy Bill to replace and modernise the Act.

In 2011, the New Zealand Law Commission (NZLC) published a detailed report on the Privacy Act, including a number of suggested areas for reform. Near the top of the NZLC's list were stronger enforcement powers for the Commissioner.

Three years later, in 2014, the Government responded to the NZLC's review of the Act, by acknowledging that privacy-related risks had changed considerably since the Act was first passed in 1993, and particularly in recent times. Technological advancements in the way in which personal information is captured, stored, and shared by both public and private sector agencies (within and across borders) have led to increased demands on the Commissioner, growing concerns about private sector privacy practices, a proliferation of underdeveloped public sector privacy practices, a loss of public trust in agencies, and continuing privacy breaches – along with an increase in the cost of, and harm that can be caused by, those breaches. In this context, the Government noted that it is socially desirable for most privacy breaches to be avoided in the first place, rather than addressing the harm caused by breaches.

The Government subsequently recommended introducing three key changes to New Zealand's privacy laws:

- First, making notification of privacy breaches mandatory. This is currently voluntary, though very strongly encouraged by the Commissioner. The Government's proposal would introduce a two-tier regime, requiring notification to the Commissioner for 'material' breaches, and notification to both the Commissioner and the affected individuals when there is a real risk of harm. This change would also, of course, bring New Zealand closer into line with a number of comparable jurisdictions where mandatory breach notification has been implemented in recent years.
- Second, the Government called for the Commissioner to have greater own motion investigative powers. This would strengthen the Commissioner's existing powers to investigate possible breaches, and increase the penalty for non-compliance with requests for information from the Commissioner.
- Finally, it was recommended that the Commissioner be given power to issue compliance notices for privacy breaches as a result of a complaint, own motion inquiry, data breach notification or other avenue.

Although the Government rejected the introduction of fines, it noted that its position on fines was out of step with enforcement practices elsewhere, and conceded that the use of fines may become appropriate if guidance and early intervention alone are not effective.

On 3 February 2017, the Commissioner released six recommendations for reform of the Act, as part of his statutory mandate under section 26 of the Act to review and report back to the Government on the Act's operation. The Commissioner noted that rapid changes in technology and data science, and significant developments internationally (particularly the EU General Data Protection Regulation) - even since the Government's 2014 response - necessitate further matters of reform.

The Commissioner's recommendations relating to enforcement are set out below:

- Granting the Commissioner the ability to require agencies to demonstrate their compliance with the Act and their privacy

management plans. The Commissioner considers this is a necessary measure for systemic issues to be identified and addressed. It would also serve to complement the mandatory breach notification obligation and the Commissioner's proposed compliance notice power. The power would allow the Commissioner to require an agency to demonstrate its ongoing compliance by:
  - establishing a privacy management programme
  - requiring a report to the Commissioner on steps taken to achieve compliance with that requirement
  - publicly reporting on its position with regard to its privacy management programme

- Introducing new civil penalties on application to the High Court for serious privacy breaches (up to NZ$100,000 for individuals and up to NZ$1m for a body corporate). Those levels would be more consistent with Australian law (among others) and comparable New Zealand laws (eg, the Unsolicited Electronic Messages Act 2007)
- Narrowing the defences available for obstructing, or failing to comply with the requirements of, the Privacy Commissioner. The Commissioner noted his experience of agencies finding it relatively easy to defend themselves against charges of obstructing or hindering the Commissioner's investigations breaches of the Act, or failing to comply with the Commissioner's lawful requirements, by relying on a 'reasonable excuse' defence contained in the Act.

The Commissioner's report and recommendations will be taken into account as part of the Government's proposed modernisation of the Privacy Act, a draft of which is expected later this year. However, with a general election to be held in September, there is every chance that privacy law reform will slip further down the Government's list of priorities. In the meantime, the Naming Policy offers the Commissioner a useful tool to encourage compliance with the Act - particularly for those organisations for whom reputational and brand impact focus the mind as effectively as legal or financial remedies.

This article was first published in the April 2017 edition of Data Protection Leader.

Mandatory data breach reporting in Australia

As noted in our article "What's in a name?", mandatory data breach reporting has been on the agenda in New Zealand for some time. While they may have some ground to make up on the rugby field, it is one area where our trans-Tasman cousins have stolen a march on New Zealand. In February this year, the Australian Parliament enacted the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) (the Amendment Act) which will (when it takes effect on 22 February 2018) require that all 'eligible' data breaches are notified to both affected individuals and to the Office of the Australian Information Commissioner (the OAIC).

The new regime will apply to all organisations that are caught by the principles set out in the Australian Privacy Act 1988 (Cth). In practice, that is a long list and will include all Australian public sector agencies, any private sector and not-for-profit organisations with annual turnover of greater than A$3m, as well as some small businesses (collectively referred to in the Privacy Act as 'APP entities'). APP entities will be required to notify a data breach if:

- There has been unauthorised access to, or disclosure of, information, or information has been lost in circumstances where unauthorised access or disclosure is likely to occur
- Objectively, that access or disclosure is likely to result in 'serious harm' to any individuals to whom the information relates.

In assessing whether 'serious harm' is likely to result, APP entities are required by the Amendment Act to:

- Consider the kinds and sensitivity of the information
- The kinds of people who are likely to have obtained access to it (and presumably, what their motives and likely uses of that information are)
- Whether it was protected by any security measures (such as encryption)
- The nature of the harm that could result.

Those factors allow APP entities a certain amount of discretion in determining how 'serious' a breach is. While it's frequently argued that immediate and voluntary disclosure following a breach is a very good thing, a significant number of breaches still go unreported in the hope of avoiding reputational, regulatory and legal damage. The same self-preservation interest is likely to remain a factor when an APP entity considers how 'serious' the harm from a breach could be, and therefore whether the mandatory notification requirements apply to them.

At the same time, the new law needs to draw a line somewhere. As pointed out at a recent IAPP breakfast seminar hosted by Buddle Findlay, leaving a computer unlocked and unattended could be argued to be a data breach so any notification regime needs to create a sensible and workable yardstick that organisations can work with.

In Australia, the OAIC has promised guidance to assist APP entities in determining the seriousness of a breach. Here in New Zealand, guidance published by the Office of the Privacy Commissioner (OPC) strongly encourages notification to affected individuals and the OPC where there is a risk of harm (note the absence of the qualifier 'serious'). In a voluntary notification

regime, organisations will exercise a lot more discretion, and so seriousness or materiality will be read into any decision on whether to notify or how to proceed.

The introduction of a mandatory breach reporting regime, and broader privacy law reform, has been on the cards in New Zealand for a long time (we've written about this previously here). While there seems to be political will from both sides of the aisle, the process of introducing those reforms has not moved quickly. When it comes to breach notification, the best indicator we have is from a May 2014 Cabinet Paper which outlined a two-tier regime involving:

- Notification to the OPC of 'material' breaches
- Notification to both the OPC and affected individuals for more serious breaches, being those where there is a real risk of harm.

While any final statutory language would need to go through the various Law Commission, Parliament and Select Committee filters, it is interesting to note that, based on the wording of that Cabinet Paper, the prospect of any harm is enough to constitute a breach as 'serious' and therefore warrants notification to affected individuals. Whereas in Australia, there seems to be a qualitative threshold applied to the nature of the harm itself - ie, a breach is only notifiable if it is likely to lead to serious harm.

To some extent, that might be playing with words, but there would presumably be advantages in aiming for consistency across the language and requirements of the two regimes. Companies operating in both the New Zealand and Australian markets could implement uniform policies and practices and there would be a greater body of applicable regulatory guidance, real-world experience and market practice available to people on both sides of the ditch, regardless of what rugby team they support.

Government procurement - balance restored

ICT procurements in the government sector can be complex and fraught. In our experience, agencies generally work hard to try to find the best solution for Government while adhering to good procurement principles (including fairness and playing by the rules). In recent years in relation to ICT projects, we've detected an increased nervousness about adopting processes which are not viewed as 'standard' or making changes to processes mid-procurement. This can include reluctance to use the flexibility already provided for within many RFP documents in a manner that could lead to better results (such as running commercial clarification sessions if responses are unclear).

Such reticence may have been in part due to a High Court decision that went against the Ministry of Health (the Ministry) in 2015, although the case did not relate to an ICT procurement. In 2013 the Ministry put out a tender for services to in relation to problem gambling. The long-time incumbent, the Problem Gambling Foundation, put in two responses but was largely unsuccessful. The Foundation took the Ministry's decision to the High Court for judicial review. The High Court reviewed the Ministry's decision against the requirements for decision-making when exercising public powers and found that Ministry's decision was deficient against those requirements.

However, just before Christmas last year the Court of Appeal in the decision of *Attorney-General v Problem Gambling Foundation of New Zealand* [2014] NZHC 213 released a decision that is likely to have been welcomed by a number of government agencies.

The Court of Appeal held that commercial decisions in the public sector are only able to be reviewed by the courts if:

- there is some extra public law feature (e.g. preventing settlement of a Treaty claim)
- the agency has failed to follow statutory requirements
- there is fraud, corruption, or bad faith.

Procurement decisions are then generally safe from judicial review, unless one of those exceptional factors applies. The Court of Appeal also determined that the test for bias which the High Court had applied was incorrect and too restrictive and that the mandatory procurement rules (now replaced by the Government Rules of Sourcing) are not legally enforceable by unsuccessful tenderers. A more detailed summary of the case can be found here. We hope that this decision may give agencies some confidence in designing processes which adhere to good procurement practices and the Rules of Sourcing but are sufficiently flexible to ensure best results.

New Ministry of Health Policy Removes Barriers to Uptake of Cloud Services

As more and more of us turn to cloud computing as a reliable and convenient way to manage our information, the Ministry of Health has overhauled its cloud computing policy and made it much easier for healthcare providers to use these services to store health information.

In the past, health care providers that relied on the Ministry for funding (like District Health Boards) could not store health information on cloud servers located overseas without first getting an exemption from the National Health IT Board. This policy enabled cautious use of cloud in the healthcare sector, but reflected the Ministry's concerns about security, integrity and

accessibility of sensitive health information.

The Ministry relaxed its policy slightly in early 2016 by pre-approving certain services, but the list of pre-approved services was quite short.

In 2017, to align with Cabinet's "Cloud First" policy, a major overhaul has been implemented (read the policy here). The list of pre-approved services and the exemption regime have been removed. The National Health IT Board has been disbanded, and replaced with a Digital Advisory Board that advises the Ministry.

Health providers are now permitted to store personal information using a public cloud service (whether in New Zealand or overseas) as long as they first undertake a formal risk assessment and have it signed off by senior management before use of the services.

Guidance on how to manage risk assessments is available on the Government Chief Information Officer's (GCIO's) website here. If the risk assessment gives rise to significant concern, the GCIO advises consulting with the Ministry before proceeding further.

DHBs are also subject to additional requirements, namely:

- Ensuring that the cloud service meets the requirements of HISO standard 10025:2015 - the Health Information Security Framework's Section 18, Cloud Computing and Outsourced Processing
- Forwarding a copy of completed risk assessments to the Government Chief Information Officer and the Ministry of Health prior to using the cloud services
- Recording each individual public cloud service utilised within its application portfolio management system.

Healthcare providers will welcome this freedom to choose services that suit them operationally. However, they also need to take care - the duty to check for risks is now their responsibility alone. Under the Health Information Privacy Code and the Privacy Act 1993, health providers have a legal duty to take reasonable steps to prevent unauthorised access, use, modification and disclosure of health information that they hold. The Ministry's new guidelines help healthcare providers to perform appropriate due diligence and make the necessary risk assessments and decisions on a case-by-case basis.

Blockchain update

Distributed ledger technology such as blockchain, the technology underlying the Bitcoin cryptocurrency, has become a buzzword almost synonymous with 'disruption' across a growing number of industries. We've been writing about the blockchain for some time ("Regulating the Blockchain" and "Smart Contracts - what are they are what differences could they make" and "Blockchain, what is it and why does it matter?"). More and more innovators are looking to devise new ways of exploiting blockchain to allow for the expedited transfer of value or data without the need for trusted central intermediaries. Some of the recent applications (and implications) of distributed ledger technology in the ever-changing blockchain space include:

- **Securities post-trade processing**: At the beginning of 2017, the Depository Trust and Clearing Corporation (DTCC) announced that it had selected IBM and two blockchain startups (Axoni and R3) to develop distributed ledger software for its post-trade processing in the credit derivatives market. This distributed ledger solution is projected to be the largest practical rollout of scale based on the technology to date and will build on the current "Trade Information Warehouse", which manages records and payments for trillions of dollars worth of credit derivatives. The distributed ledger, which operates as a single source of truth, will address a shortcoming of the current system, namely that the post-trade data is entered into multiple databases in different ways. However, the rollout, which is currently planned for 2018, does come with an important qualification - participation in the network will be voluntary for the more than 2,500 buy-side firms that use the current system, which means that the need to reconcile multiple ledgers will still exist, at least initially. DTCC chief executive Michael Bodson conceded that this situation "doesn't take advantage of the end-state, which is one version of the truth, but it's a step in that direction" (Read the full article here)
- **Digital fiat currency**: In 2014, approximately a year after the Bitcoin values skyrocketed and the world began to take notice, China's central bank established a research team to look into the development of a government-controlled cryptocurrency. As of early 2017, the People's Bank of China (PBOC) had conducted trial runs of its prototype digital currency. For consumers transacting through smartphones and other devices, the change from physical currency to the central bank issued cryptocurrency probably would not seem much different, although it would reduce transaction costs for merchants by removing some of the banks and other payments provider intermediaries. However, the potential systemic advantages for the government are substantial, such as allowing the PBOC to monitor risks in the financial system and creating the potential for the collection of "real-time, complete and authentic" data to an extent scarcely before imagined. Other countries are also looking at launching digital versions of fiat currency, including Canada (with CAD-COIN) and the United Kingdom
- **Privacy implications**: The New Zealand Privacy Commissioner, John Edwards, recently shared some interesting thoughts on the implications that blockchain can have relating to privacy. Specifically, blockchain will allow individuals to control their own data in unprecedented ways, which could potentially nip the burgeoning trend of monetizing personal data in the bud. However, he raised some risks, such as whether the immutability of the blockchain would mean that it was impossible for

individuals to get their personal information deleted or amended – given that the core concept of a blockchain is that it is a permanent and transparent ledger (Read the full article here)

- **Supply chain optimisation**: Some companies, including Foxconn (one of the world's largest tech employers) are now looking into using blockchain to minimise the frictions that arise in manufacturing supply chains due to funding delays. Foxconn's project, separately incorporated as Chained Finance, aims to onboard entire supply chains so that loans can be paid directly to the manufacturer in need, without having to pass these loans down the chain. This is particularly advantageous in industries where some supply chains can run 13 'links' deep, and such delays have the potential to stop work or even close factories. The blockchain platform would work by core suppliers handing over their supply chain data to Chained Finance, who would then onboard the other members of the chain, giving each credentialed access to the blockchain platform. Payments would then flow through the chain as and when necessary with minimal delays, with all the information being recorded on the private ledger.

There still exist many regulatory hurdles that blockchain developers and adopters will need to overcome as the rollout of new applications becomes more widespread and Governments are still considering how to approach this new technology and its implications on the existing regulations. In the UK, the Financial Conduct Authority is currently circulating a discussion paper seeking views on the potential future of distributed ledger technology in the markets that it regulates. In March 2017, the Arizona state legislature voted to pass a bill giving legal status to smart contracts and blockchain-based signatures, meaning that the current contract law applies to blockchain-based contracts. The law also states that blockchain based data amounts to ownership, which acts to clear up any residual ambiguity as to what may amount to theft in the blockchain space. This is the first legislation of its type globally. (Read related article 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