



ADLSI

Independent Voice of Law

LAWNEWS THIS ISSUE:

Welcome to our special “Technology & Law” edition, put together by ADLSI’s Technology & Law Committee.

We hope you enjoy it!

LAWNEWS

SPECIAL ISSUE TECHNOLOGY & LAW

ISSUE 29 26 AUGUST 2016

www.adls.org.nz

+ *Law and virtual gaming*

POACHING POKÉMON IN THE VIRTUAL ESTATE

By James Ting-Edwards, Issues Advisor, InternetNZ

For the uninitiated, “Pokémon” are fictional “pocket monsters”, which first appeared in video games 20 years ago. Now these virtual creatures are in our streets, parks and offices, thanks to a smartphone near you.

The game “Pokémon Go” was released on 6 July 2016, initially in Australia, New Zealand, and the United States. It has been astonishingly popular, with more than 100 million downloads in less than a month. Through smartphone location and camera functions, Pokémon Go creates an “augmented reality” (AR), which combines real-world and virtual elements. Location functions support an “exploring” component, which relates real-world locations to in-game features – “Pokéstop” locations with free supplies, Pokémon which can be found and captured, and gyms which can be fought for and controlled.

Finding a nearby Pokémon triggers a “catching” mode, which presents the capturable creature on-screen, overlaid on a player’s real-world surroundings. In this way, the game creates a window onto a virtual world neighbouring our own. The combination of massive popularity with novel exploring behaviours results in potential social and legal issues. There are privacy implications – the game is free to play, but collects valuable data on players.

Those who logged in on Apple devices, using Google accounts, were initially asked for “full access”, implying an ability to read contact



“Pokémon Go” – the attraction of distraction can be a nuisance.

information, email, and everything else therein. Fortunately, in this case “full access” was not given – this inaccurate term survived from older versions of the log-in process. This is not very reassuring, given that many players accepted the asserted intrusion into personal data.

Perhaps most interesting are the interactions between the game’s virtual features, and the real-world locations to which they correspond. A player’s quest to “catch them all” may mean walking or driving through places which were previously neglected, private, or solemn. Some institutions (including the Courts of New South Wales) have asked players to “go away”, at least where phones are prohibited as recording devices. Absent contract, it seems doubtful that there is a legal basis for excluding players from these locations. Even in private places, the law of trespass provides an implied licence to enter

for a lawful purpose. On the other hand, the consequences of individual behaviours depend on how common those behaviours are. Things which are benign when done by a few people may become harmful when done by thousands. Does the game’s maker, Niantic, create a nuisance by attracting distracted players where they are not wanted?

For good or for ill, popularity also leads to opportunistic behaviours. In-game, players can purchase items for real money, including “lures” to attract more Pokémon. Tech-aware bars and cafés have used these lures to attract players. Some promotions have gone further – an Auckland jeweller offered a free gemstone to any player who had captured the “Starmie” Pokémon. On the less positive side, eager and distracted players may be vulnerable to real-world crimes.

Continued on page 2

POACHING POKÉMON IN THE VIRTUAL ESTATE

Continued from page 1



James Ting-Edwards

By gathering user data, or simulating clicks on

In O'Fallon, Missouri, a group of armed men used in-game "beacons" to lure players and rob them. In regions where official access to the app was delayed, similarly-named applications sprung up to take advantage of eager downloaders.


advertising links, these scam applications turn unpleasant experiences into unearned revenue.

Pokémon Go is the first massively popular augmented reality app. It demonstrates that smartphones and other technologies will find new uses, and create new patterns of behaviour, with new social and legal consequences. Pokémon Go offers a window into a neighbouring reality, but also a mirror on human behaviour, good and bad.

Further reading:

- Paul Hill, "New South Wales courts tell Pokémon GO players to go away"

(<https://www.neowin.net/news/new-south-wales-courts-tell-pokemon-go-players-to-go-away>).

- K. Amani Fine Jeweller, "Pokemon Gemstone Madness" (<http://www.kamani.co.nz/pokemon-gemstone-madness/>).
- Sam Machkovech, "Armed muggers use Pokémon Go to find victims" (<http://arstechnica.com/gaming/2016/07/armed-muggers-use-pokemon-go-to-find-victims/>).
- Sarah Perez, "Beware the fake Pokémon Go apps" (<https://techcrunch.com/2016/07/18/beware-the-fake-pokemon-go-apps/>). 

Doctor's orders? Storing health info offshore



Edwin Lim

By Edwin Lim,
Partner, Hudson
Gavin Martin

Up until a few months ago, the National Health IT Board's guidance ("Use of Cloud or hosted services for managing health information") stated

that any health care provider holding personal health information in an identifiable form must have that information fully domiciled in New Zealand, unless an exemption is granted to that provider by the IT Board.

We have spoken to a number of concerned providers, as they already hold personal health information in (world-class) data centres or cloud based storage services located outside New Zealand. Why have they made that decision? Lower costs, scalability and, importantly, the exceptional level of security that many overseas data centres and cloud-based storage services are able to offer.


So, should health care providers be concerned about the requirements of the IT Board's guidance? Well, it depends. In my view, the guidance is somewhat unclear. I am not aware of any legislation that requires cloud storage of personal health information to be domiciled

in New Zealand, yet the guidance is drafted in mandatory terms. Yes, we have the *Privacy Act 1993* and the *Health Information Privacy Code 1994*, but there is nothing in the Act or Code that makes it a legal obligation for personal health information to be domiciled in New Zealand. At best, I think the guidance is in place so that health care providers can act in a manner that follows good or best practice. That said, there are compelling reasons why a health care provider might want to "comply" with the guidance.

First, a government-funded provider, or a provider providing services to a government-funded customer, may need to comply with the guidance as a requirement of the relevant entity receiving funding. Second, it would be complying with a guidance issued effectively by the Ministry of Health, so that is a big tick in the eyes of the Ministry, patients, and customers. Third, if it seeks an exemption and it is granted, then at least it can be satisfied that its due diligence process on the overseas data centre or cloud-based storage service was good enough for the IT Board (among other considerations) in granting the provider an exemption. However, one further issue for providers to bear in mind is that, if an exemption is granted, along with annual privacy and security audits of the relevant service, they will also need to maintain a copy or back-up of all personal health information held in an identifiable form,

domiciled in New Zealand.

I started this article with the words "up until a few months ago". It is pleasing to see that the IT Board has recently updated its guidance so that health care providers will not need to seek an exemption to hold personal health information overseas where they are using a product or service that the Ministry has "accepted" as "fit for purpose". So far, products and services "accepted" by the Ministry as "fit for purpose" are Oculo, Gallagher Bassett, Azure, Office 365 and Dynamics CRM (Microsoft), and Infosmart Web (Fisher & Paykel Healthcare). I am sure that a number of other hosting or Cloud service providers will appear on that list soon.

Developments in the health IT sector in relation to the use of overseas Cloud or hosted services may influence the creation of policies, regulations, codes or even legislation that may one day apply to businesses in other industries (including law) that use similar services. Government agencies that wish to use Cloud-based services are already required to comply with policies and risk assessment procedures put in place by the Government Chief Information Officer (GCIO). The GCIO is also certifying certain suppliers as having cloud services that government agencies can have confidence in. Given the cross-over, the GCIO and the Ministry are working to align the two certification/acceptance processes. Watch this space! 

LAWNEWS

LAW NEWS is an official publication of Auckland District Law Society Inc. (ADLSI).

Editor: Lisa Clark

Editorial and contributor enquiries: Lisa Clark, phone (09) 303 5270 or email lisa.clark@adls.org.nz

Advertising enquiries: Chris Merlini, phone 021 371 302 or email chris@mediacell.co.nz

Law News is published weekly (with the exception of a small period over the Christmas holiday break) and is available

free of charge to members of ADLSI, and available by subscription to non-members for \$133 plus GST per year. If you wish to subscribe please email reception@adls.org.nz.

All mail for the editorial department to: Auckland District Law Society Inc., Level 4, Chancery Chambers, 2 Chancery Street, Auckland 1010. PO Box 58, Shortland Street, DX CP24001, Auckland 1140. www.adls.org.nz

There is a regular practice of photographing people at collegial events and some of those photos are published in *Law News*. If you are attending such an event and you do not wish to have your photograph taken, please tell the photographer and your request will be respected.

©COPYRIGHT. Material from this newsletter must not be reproduced in whole or part without permission.

Block chain technology and licensing



By Melanie Johnson, ADLSI Technology & Law Committee Convenor and legal counsel at the University of Auckland

Does block chain technology spell the death knell for blanket licences and

will it allow for a potentially cost-effective means of licensing copyright content, which could see copyright owners more fairly remunerated?

Reproduction Rights Organisations (RROs) license the reproduction of material protected by copyright whenever it is impracticable or impossible for rights holders to act individually. In New Zealand, RROs operate under a voluntary licensing model and issue licences to copy protected material on behalf of those rights holders who have mandated it to act on their behalf. The New Zealand RROs are: Copyright Licensing Ltd (CLL), which licenses the copying of books and journals; the Audio Visual Copyright Society, known as Screenrights, which licenses the copying of communication works which are films; and APRA/AMCOS and PPNZ, which license music. RROs generally obtain licensing authority for international repertoire through bilateral agreements with RROs in other countries. These bilateral agreements are based on the principle of reciprocal representation. Screenrights on the other hand deals directly with copyright owners or their agents.

While RROs may issue transactional licences, generally New Zealand RROs issue blanket licences which cover all uses of their works by members of the licensee. The rationale behind the development of RROs is that licensing reproduction cannot function effectively on an individual basis. Mandates are acquired either on an individual basis for music and film or from rightsholders' associations, such as the Society of Authors, and Publishers Association in New Zealand.

A case filed in the Federal Court of Australia highlights some of the problems for RROs and their members. Earlier this year, the Australian Writers' Guild filed a case against Screenrights over its failure to fairly protect and represent Australian and international scriptwriters and their rights. The Guild asserts that Screenrights "appear[s] to have collected over \$50 million in script royalties over the past 20 years, yet the Guild's Australian members may have received as little as \$350,000". The difficulty for Screenrights is in determining who the rightful owner is. A claimant may be a writer, director and a producer, or there may be arrangements between writers and producers whereby producers claim secondary royalties (such as Screenrights' royalties) and then provide writers with a share of the backend. Screenwriters and writers' agents are also able to claim royalties direct from Screenrights rather than through a

writers' guild collecting society.

In a blanket licensing approach, the RRO sets the price members receive for use of their work. As Vincent O'Donnell from RMIT explains, payments for film rights are calculated on a point value system which is based on the nature of the programme, the duration and number of copies made and the uses of the programme. This point score translates into a share of the money pool that is ultimately distributed to rights holders. Generally, the top copyright is vested in the producer. How the royalty is divided up between the various creatives is set in the contracts and relies on the producer to administer and ensure the appropriate payments are made to rights owners. This system works not just for Screenrights but for all RROs who will pay the producer or publisher, who then distribute to their authors. All arrangements with the principal creative workers are contained in the individual contracts with the producer.

While the fees paid by licensees are significant, it is difficult to record every use of a work in a large, fragmented and highly-institutionalised market such as the education sector, which is Screenrights' main market. Traditionally, surveys of usage report only a snapshot in time of usage – they are costly, time-consuming and generally rely on staff self-reporting use, so are often inaccurate. RROs in New Zealand are moving away from this model and looking at alternative means of recording usage to enable more accurate payment to their members.

Block chain technology may have the potential to solve some of the problems of blanket licences, by automatically recording usage and ensuring rights owners are paid for each use of their work. A block chain is a type of distributed ledger, comprised of unchangeable, digitally-recorded data in packages called "blocks". Each block is then "chained" to the next block, using a cryptographic signature and what is now known as a "proof-of-work consensus algorithm". This allows block chains to be used like a ledger, which can be shared and accessed by anyone with the appropriate permissions. This creates an immutable "World Wide Ledger". This digital ledger can record who owns property, and provides a complete ledger of every transaction ever made in relation to that property. The evidence and the chain of activity cannot be circumvented and the record exists forever.

Like the World Wide Web, this ledger is not owned or controlled by any company, individual, or government. It is shared peer-to-peer across thousands of computers all over the world. Its accuracy is greater than the self-reporting described above. Block chain can deliver an accurate granular record of use and therefore payment entitlement. The ledger allows the creation of incorruptible "digital tokens" that represent information on this World Wide Ledger. The information on the digital token can represent things like an identity, a public record, a housing title, a car title, a stock in a company, a bond, a social media profile, a book, and ownership of intellectual property.

Whoever has the digital keys to unlock this digital token can claim ownership of that digital token, and can transfer it from one person to another. Management of tokens and digital keys requires software that you can download into a "digital wallet" which can be stored on your phone or other device. When a person uses their digital keys to unlock and send a digital token they own to someone else, the transaction is recorded on the World Wide Ledger (and that digital key can no longer be used to control that token). Now the recipient has control over that digital token and has the digital keys to control it.

Smart contracts programmed using the parameters set by the parties and run on custom-built block chain platforms (such as Ethereum) could be used by the multiple rights owners in a film or other works. RROs set the price and the block chain creates a visible record of all usages to ensure rights owners are paid. This could well solve the sorts of problems faced by Screenrights and other RROs. The RRO or an individual licensor can create a smart contract to lend this digital token for a certain period, depending on what the parties agree to. On execution of the contract, access to the content is granted. Whenever the work is accessed or copied, that use is recorded in the ledger and payment would be made at a predetermined time or event, for example when a minimum payment threshold is reached.

For users in a multiuser corporate environment, each licence entitlement requires a unique address belonging to the organisation to be sent a token, with multiple addresses defining the number of tokens the organisation has available. An organisation such as a university with over a thousand teachers and 20,000 students pays blanket licence fees based on the number of students enrolled in the institution. However, the use of learning analytics suggests that often only very few of those students access the content. This would allow a university to pay on the basis of the number of addresses in a wallet dedicated to that licensed content. The licences can be allocated to users within the institution and can also be revoked. The licence could set rules for users, recorded in the smart contract, for example, that content can only be made available to students enrolled in a particular course via the institution's learning management system (LMS). The digital key to unlock the content would not work outside the LMS. Users would need to authenticate using the institution's login credentials, using a single sign-on approach to access the licence from the institution's wallet.

This system would work for other rights management. A digital token representing a book, film, or music can be used to create smart contracts with different people or organisations. An author can create a token that represents his or her work on the World Wide Ledger. While the work itself is not viewable on this ledger, the digital fingerprint that proves ownership is. This allows for the creation of a smart contract with

Continued on page 13

ADLSI's Technology & Law Committee

Innovation lies at the heart of our changing world. From government policy to the practice of law, technology creates amazing opportunities and daunting challenges. The ADLSI Technology & Law Committee (Committee) sees itself as having a mandate to keep up-to-date with the times and offer relevant perspectives on topics such as modernising legal processes, electronic discovery rules, privacy, intellectual property, online safety, cyber-crime and cloud services governance.

In this third annual special "Technology & Law" issue of *Law News*, the Committee continues its focus on providing practitioners with articles and advice on the impact that new technologies are having on law and legal practice.

The Committee has a keen interest in the development of law and policy with a technological aspect. Members maintain a watching brief and make submissions on new pieces of legislation and government policy in relation to the use and security of technology and data security.

Recognising that technology has the potential to impact a whole raft of different legal practice areas, the Committee Members bring together a wide range of backgrounds. Current Committee Members are:

Melanie Johnson – Heading up the Committee is Committee Convenor Melanie Johnson. Ms Johnson is legal counsel at the University of Auckland. She is part of the Corporate Services Team in the University library and advises the University on copyright. She is a member of the Copyright Negotiating Team that negotiates copyright licences on behalf of all New Zealand Universities. She has a particular interest in copyright and the impact of technology on the way in which copyright material is being generated and used. She can be contacted at mf.johnson@auckland.ac.nz.

Mark Donovan – Mark Donovan is a barrister specialising in employment-related matters and disputes (including mediation, appearances before the Employment Relations Authority and the Employment Court, and advising on employment agreements), as well as acting in relation to other civil disputes (including liquidations, restraints of trade, confidential information and regulatory investigations). He has a keen interest in adopting technology that enables lawyers to increase efficiencies in their legal practice and deliver better value for clients. He can be contacted at mail@markdonovan.co.nz.

Andrew Easterbrook – Andrew Easterbrook is a senior lawyer at Webb Ross McNab Kilpatrick in Whangarei. He works in the dispute resolution team, dealing mainly with technology law, civil litigation and contentious relationship property disputes. He is also a musician and a computer geek. He can be contacted at andrew@wrmk.co.nz.

Lloyd Gallagher – Lloyd Gallagher is actively involved around the world in alternative dispute resolution where he acts as an arbitrator and mediator. With a strong IT background, he works with law practitioners and policy makers to develop solutions that focus on access to justice and technology security. His research focus and consultancy range from technology law, equity, condo disputes, international contracts and tax to regulatory policy, through Canada, the UK and Asia Pacific. Mr Gallagher can be contacted at Lloyd@gallagherandco.co.nz.

David Harvey – David Harvey was appointed as a District Court Judge in 1989, and sat at Manukau for 20 years before transferring to Auckland in 2009. Since his appointment to the bench, Judge Harvey was closely involved with information technology initiatives involving the judiciary including the development of trial management software. He recently stood down from the Bench and is now the Director of the New Zealand Centre for ICT Law at the Law School at the University of Auckland. He can be contacted at djhdcj@ihug.co.nz or david@internetlaw.nz.

Arran Hunt – Arran Hunt is a solicitor at Turner Hopkins. Mr Hunt has previously worked as a technical business analyst for a Fortune50 company in London and several large firms and city councils in Auckland, before being admitted in 2010. He has an interest in the interrelation of technology with law and business. He can be contacted at arranhunt@turnerhopkins.co.nz.



Members of ADLSI's Technology & Law Committee: (back row, from left to right) Mark Donovan, James Ting-Edwards, Arran Hunt, Melanie Johnson; (front row, from left to right) Ellie Ryan and his Honour Judge David Harvey. Not pictured: Andrew Easterbrook, Lloyd Gallagher, Edwin Lim, Daniel Wong and Callum Burnett.

Edwin Lim – Edwin Lim is a partner at Hudson Gavin Martin, a boutique commercial and corporate law firm specialising in technology, media and IP. He has specialised in these areas for over 15 years. With two Honours degrees in Law and Commerce (Management Science and Information Systems), he understands the commercial, technical and legal issues involved in a client's project, and is comfortable talking to clients about complex technology matters. He is also currently involved in moving his firm's technology systems into a Microsoft Azure and Office 365 environment. He can be contacted at edwin.lim@hgmlegal.com.

James Ting-Edwards – James Ting-Edwards leads InternetNZ's policy work on law and rights issues. In practice, this means fuelling and informing discussions between people in technical, legal, and other communities. Mr Ting-Edwards draws on experience advising start-ups on IP issues, and teaching at the University of Auckland. Outside work, he enjoys gardening, gaming, and improv theatre. He can be contacted at james@internetnz.net.nz.

Daniel Wong – Daniel Wong is a co-founder of Flacks & Wong Limited, a specialist corporate law firm. Mr Wong has advised listed and private companies, entrepreneurs and start-ups in the technology sector on their corporate, capital markets and commercial transactions. Flacks & Wong has adopted a wholly cloud- and Saas-based legal practice management system. He can be contacted at daniel@flackswong.co.nz.

Technology & Law Committee Equal Justice Project (EJP) student representatives, Callum Burnett and Ellie Ryan – Callum Burnett and Ellie Ryan represent the Equal Justice Project or "EJP" on the Committee. The EJP is a student-run pro bono initiative based at the University of Auckland's Faculty of Law. The EJP works with practitioners, non-profits and the general public to increase access to the law and promote legal awareness in the community. Callum and Ellie are law students in the final stages of their degree, with a keen interest in how technology can enhance access to justice and empower individuals to gain legal knowledge. The EJP can be contacted at directors@equaljusticeproject.co.nz.

The Committee welcomes any comments or questions – any correspondence should be directed to ADLSI Professional Services Manager and Committee secretary, Jodi Libbey, at jodi.libbey@adls.org.nz.

“Sentencing by computer”?



Ellie Ryan, one of the ADLSI Technology & Law Committee's Equal Justice Project (EJP) student representatives, considers how the use of technology might assist in delivering consistent sentences for like offenders.

As early as 1983, researchers at Erasmus University in the Netherlands created the programme “SENPRO” that experimented with computers issuing criminal sentences. They concluded it was “definitely possible” for a computer to make coherent legal decisions. Legal reasoning, methodic and principled, resembled calculation in many ways.

Over 30 years later, it is more common to find suspicion about trusting computers to “make” law. A sentence calculator, no matter how desirably framed, cannot compete against a human arbiter with ethics and social expertise. But problems with the latter’s discretionary judgement – especially when a “too-lenient” sentence attracts publicity – can see surges in support of formulaic approaches to sentencing.

Disagreement about the policy and philosophy of sentencing often centres on whether the right compromise is struck on a “discretion/consistency” continuum. Though we think it fair that similar offenders receive similar sentences, it is necessary to take some account of the vagaries of life, otherwise judges may feel they have had their hand forced to impose inappropriate or unsuitable punishments. The balance usually tips toward greater discretion for the judge. If there is a significant miscarriage, then the appeal process provides a remedy. But there have been pushes for an appropriate method to bring sentencing “into line”.

Australian courts have firmly supported “intuitive synthesis” – when a judge confronts an offender and passes sentence upon them (see *Makarian v R* [2005] HCA 25, (2005) 228 CLR 357 per McHugh J). As such, they have rejected measures that might aid the decision. In contrast, the United States has taken a formulaic approach. The US Sentencing Commission publishes a “Guidelines Manual” (the most recent of which can be found at <http://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2015/GLMFull.pdf>). Although this can read like an unlikely board game (the sentencer is directed to move up one or two levels, depending on severity), but it is nonetheless incredibly comprehensive (almost 600 pages in length). One lawyer has exploited the prescriptiveness of the approach and created a freely available “Sentencing Calculator” (www.sentencing.us), where ticking the features that apply gives you some approximation of the prison time you might face.

The United Kingdom has opted for a Sentencing

Council, which considers appropriate sentences and can alter these in response to changing public opinion. Judges use guidelines to arrive at a final sentence. New Zealand attempted to institute a similar Council (some years before the UK Council). Our Law Commission’s 2006 report, “Sentencing Guidelines and Parole Reform” (11 August 2006), mentioned its disappointment in the guidance that was provided by the *Sentencing Act 2002*. The purposes and principles in the Act, being “non-prioritised and non-exhaustive”, had little intelligible bearing on judges’ actual decision-making. Only high-level offences were dealt with at appellate level, leaving a dearth of guidance for lower courts. The Commission recommended a Sentencing Council be established, but a change in government shortly thereafter meant the empowering Act sat impotent on the books.

New Zealand’s key method for sentencing consistency has come from within the judiciary itself in the form of “tariff” or “guideline” judgments, the best known being *R v Taueki* and *R v Mako*. The sentencing “bands” they identify are flexible and overlapping. Yet, as the Commission rightly identified, these judgments are concocted for higher-level offences, neglecting the bulk of less-serious offences dealt with by District Courts. So, if a Sentencing Council in New Zealand has not come to fruition, why might we look at technological tools, particularly to direct judges on “lesser” offences? We can mean different things when talking about “sentencing technology” tools. A tool might purely be an information resource or database – a means of aggregating past decisions to provide a better picture of the common law. This is likely to be less objectionable than a tool that generates the sentence itself. But such a tool, yielding a standalone preliminary judgment, is worth discussion.

It is acknowledged that the very idea of technology for sentencing generates mistrust. Computer prediction, it is said, cannot replicate individual judgement – it will fail to appreciate human nuance and to adjust itself accordingly. But consider the extent to which data is used in criminal justice already. Actuarial risk prediction is increasingly common, and tools like “RoC*RoI” (Risk of Conviction, Risk of Imprisonment), that rely upon demographic and static predictors of criminal behaviour, are used by Corrections to help identify high-risk individuals. In light of this, there are three key arguments for a sentencing tool divorced from human judgement.

1. Increasing consistency

A critique of computers is that they lack empathy. Sentencing in human hands has the benefit of human impact and connection. But we might think that this forms part of the problem. The “feel” of a case is bound to be an unconscious influence on the sentencer. New Zealand has never been praised for equitable racial proportions in its prisons, especially when considered in conjunction with gender


– it would be interesting to see how cases were treated when examined through a technological lens. Technology is nothing if not forcibly impartial. Another variable in sentencing is geography – where the sentence is delivered. Empirical studies show serious disparities in sentences handed down for the same crime in different localities (see Goodall, “Sentencing Consistency in the District Courts”, PhD Thesis, Victoria University of Wellington, 2014).

2. A basis of appeal

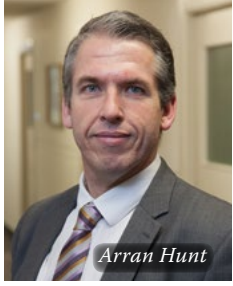
Judges are encouraged to segment their sentencing notes and differentiate between grounds that give rise to a lesser or greater sentence. This makes it easier for appellate judges to examine lower court decisions. But the facts of the case can interfere, making the sentence at first instance inscrutable on later examination. Where a sentencing tool aids the process is by generating a discrete result that is a “starting point” in itself. A judge would then be compelled to explain the reasons why he or she thinks the result is fair or otherwise. These reasons could be examined on appeal and used by counsel to advance arguments. This has advantages over the “guideline judgment” methodology. If someone is given a range (or “band”) and asked to shoot a dart somewhere within it, soliciting an explanation as to why it landed where it did is near to impossible. But place the dart for them, and this provokes passionate argument and justification.

3. Connecting with the public

New Zealand’s current sentencing practice is not a matter of general knowledge. The first time someone would be likely to learn about it would be if facing sentence themselves. This is where the structured US approach might be advantageous – it makes the process easy to understand, widely accessible and more transparent. But is there such thing as too much transparency? Some argue reducing sentencing to straightforward rules makes punishment too predictable. Taken to absurd lengths, it might mean a prospective offender makes a few calculations and chooses one of the less-serious weapons, just to shave a few months off the final sentence.

Whether or not these arguments have merit, they can spark interesting debate. Perhaps it is time to consider some method, potentially technological, to address the disparities that still exist. The sentencing stage is probably the most amenable to technological aid – more so than ruling evidence in or out, or entering a conviction. There is no basis to think that such tools would render judges obsolete – at the very least, they could aid in what are undoubtedly complicated exercises. If a sentencing tool were to be developed, the proper weight to be given to it is another question. The result might be treated as a recommendation, or as binding with a measure of departure permitted. These questions are left open here, and maybe only in practice would such a tool’s workability become clear. 

Human hacking – “phishing” and “vishing”



By Arran Hunt,
Turner Hopkins

Computers have become central to almost every business. The ready access to information demanded by users and clients has led to more information at your fingertips than

ever before. As a result, the security on that information is increasing.

With the occasional exception, our networks and data are the safest they have ever been. However, there is still one major security flaw present in every system – no matter what security we put in place, the information is still accessible to the users. Staff need to have access so that they can do their job. As digital security has advanced, so have the techniques used by hackers. One of those is a technique called “social engineering”.

The early days – mass emails

The first social engineering that you will most likely be familiar with is the emails from Nigerian princes in need of help. It provided the lure of easy money for very little work, relying on the user’s greed. All that was required (once they reeled you in) was some of your money to help release their millions. Of course, those millions would never arrive. They soon moved to faking emails from banks and courier companies, trying to get you to enter bank account details or courier release fees in a process called “phishing.” At first, they were easily spotted fakes, using free email services and riddled with spelling mistakes. Over time, they improved, taking on the look of genuine company emails. Through hidden websites, hackers are even able to purchase company email and invoice formats, making faking authentic emails that much easier, as they are identical to the real thing. While only a small percentage of recipients ever believed these emails, the technique was profitable for hackers based purely on the huge number of emails sent out.

Hackers also began using phone calls to find targets. Instead of an email, the caller will be running through a script, in much the same way as a salesperson does. The simplest methods often involve an attempt to get people to install dangerous software onto a PC, allowing the hacker to take control (and then ransom it back). The PC could then be used to attack other PCs, to monitor use for information such as bank account logins and passwords, or to ransom back to the user. Many people would have received a phone call from someone purporting to be from Microsoft. They would say they were providing a “courtesy call” about a virus infestation that the user’s PC has. They would direct the user to a website to download and install a programme, giving the caller control of the PC. This is a relatively common scenario which has struck a number of businesses, including one major luxury retailer in Auckland (which fortunately called the author just before the software had finished installing!).

Personalised service

More recently, there has been a shift in the method of these attacks. People were becoming more cautious, so hackers needed a new approach to gain the user’s trust. The simplest method was to personalise the message. This is relatively easy to do, due to the volume of data we now put online. Due to the time it takes, the number of targets that can be approached at once is limited. However, attacks could lead to a greater return. Similarly, attacks could be tailored to target the accounts of high value individuals, or even at the request of third parties. The information found online could start with the very basic. People will often use their mother’s maiden name or the name of a pet as a security question answer. Information that only close friends would have previously known is now available to a much larger audience. It also provides details of your connections and relationships. A hacker can see who your friends are, common interests, time spent together and how long you have been friends, etc. From these, a hacker could create a false sense of trust.

Example

Here is a simple example that a lawyer may encounter. A new client comes to you stating that they have been referred to you by an old friend of yours, their new partner. They have seen your Facebook account and found someone who appears in a number of your photos but not many recently, perhaps an old school friend who you know well but do not see often. They see that the person is in a new relationship. They have gone over your friend’s Facebook so are aware of the current news and events in their life including any highs or lows, and possibly a few things that you might not be aware of. During their phone call with you, they talk about your friend, the love of their life, gossip a little about what your friend is up to, how highly they rate your legal skills, etc. From this, they create a rapport with you. They may ask you to handle a small matter for them, for which they will quickly pay the invoice. They are getting you to lower your guard a little more than you normally would for a person you have never met. However, believing this is your good friend’s partner, you may do so without realising it. Their email address looks genuine (it is not hard to open an email account in somebody’s name), they emailed you a scan of their passport (easily altered on a PC) and they sent pictures from a holiday resort you know your friend went to (easily obtained by visiting the resort’s Facebook page). Everything here can be discovered or created very quickly with little skill required, and, without you realising it, you may be providing them with information or access that you ordinarily wouldn’t, especially to someone you have never met.

The professionals using this technique provide an even better example. Kevin Roose from Real Future asks the people at the world’s largest hacking conference to show him how it is done (check out <https://goo.gl/Yb3i3U> Real Future Episode 8 – watch from 1:30 for an impressive real life example of “vishing”).

Continued on page 7

Advice for law firms

1. If you get a referral from an unexpected source, mention to the new client that you will contact the source to thank them. However, this may not be practical if they are coming to you for advice on a sensitive matter. Remember that our clients expect confidentiality.
2. If they say they are local to you, ask them to call in to the office. They can bring original ID while they are there (we keep a scan of client’s passports in our electronic document management system, noting the date and who sighted it, in case a certified copy is ever required).
3. Ask for a retainer, and get the retainer replaced when it is used up. Do not get caught by a small retainer being paid early on only to be stung later for a lot more.
4. Get a phone number and call them back.
5. Check their social media. This might give you an idea of who they are and could show holes in their story. If anything does not add up, mention it to them.
6. Uplift their previous file from their old solicitor. You may need access to their old files so ask them to sign an authority to uplift. If you need to review their old file and they refuse to allow an uplift without a valid reason, then you may need to ask more questions.
7. If things do not feel right then run it past someone else, such as another solicitor. When they spoke with you, they would have been using emotive language, possibly without you realising. Give the facts to the other solicitor without the emotion.
8. Keep records of conversations and, if in doubt, email them a copy. If there was something discussed by phone, ask them to email you a breakdown, or email them what you believe your instructions are and ask them to confirm. This may help you structure your own thoughts without the emotive context. It could also help you show a basis for any actions should they be questioned at a later date.


Continued from page 6

Advice for clients

1. There should be procedures in place for verifying a user. They should be adhered to. If they do not exist then they need to be developed.
2. If a user is unsure about a request received over the phone then they should put the user on hold and run the situation past a colleague or manager. This will help remove the emotive context from the request.
3. There will often be a phone number on file for the user. Feel free to call that number to confirm the request. Do not change that phone number unless the user's identity is confirmed.
4. Ask the users about details of their account that would be difficult for others to know. For example, a bank may ask about recent purchases on a credit card, including the amounts and locations.
5. Do not let the caller choose the method of identification. Even if they offer a wealth of information, this may be the information they have access to. Stick with the set identification procedures.
6. Any changes to the control of or access to an account should only be allowed when the user has passed all security checks required.
7. It is better to be over-secure than under-secure – better that a customer is a little annoyed about having to answer a few questions than furious at having their account accessed by a hacker.

The only way to stop such threats is to remove everyone's access to any information. This, however, is not an option. So it needs to be about users using common sense and caution. It is easy to say that users should not trust anything

that is not backed up with evidence. In reality, expecting clients to provide every original document or prove every statement would make our roles difficult to perform. So instead, consider the few simple ways I've suggested

in the accompanying tables to help reduce the risk for both your firm and your clients. These ideas will (hopefully) get firms thinking or what measures can be taken. 

+ Law, technology and legal education**“Start-up” aiming to transform legal education**

By Callum Burnett, Technology & Law Committee Equal Justice Project (EJP) student representative

Specialising in investigating the implications of information and communications technology (ICT) within the context of the law, a new “New Zealand Centre for Information Communications Technology Law” was recently launched at the University of Auckland’s Faculty of Law.

His Honour Judge David Harvey, who recently stepped down from the bench after 27 years as a District Court Judge, is the inaugural Director of the Centre, which he describes as “a start-up”. It aims to allow students, researchers, lawyers, ICT specialists and companies to work together to identify the legal ramifications surrounding the challenges and opportunities of cyberspace. The Centre’s three main aims are teaching, research and the development of an electronic moot courtroom. Professor Andrew Stockley, Dean of the Faculty of Law at the University


of Auckland, spoke about the importance of legal education and practice staying up to date with technological developments. He recalled recently sitting in an English court as a judge’s guest, where the judge had relied on a lawyer’s mobile phone to read evidence missing from the proceeding. He hoped that the use of technology would also reduce the number of document-filled suitcases dragged past the Law School by busy litigators on their way to the High Court.

Despite still being in its infancy, two projects at the Centre are already underway. First, research into the *Harmful Digital Communications Act 2015* has seen cooperation between the Police and the Centre in a critical examination of the surprisingly high number of prosecutions under the Act since it came into force, with Judge Harvey due to attend the first defended prosecution the day after the Centre’s launch function. The second area of research is into online resources for self-represented litigants. The Centre is working collaboratively with the



Dean Andrew Stockley, his Honour Judge David Harvey and the Rt Hon Sir Anand Satyanand

Pro Bono Team of the Law School’s student-run Equal Justice Project (EJP), with the aim of discovering what resources are available to litigants in person overseas, and how such resources could look in New Zealand.

For more information about the New Zealand Centre for ICT Law, Judge Harvey is happy to be contacted at dj.harvey@auckland.ac.nz. 

+ ADLSI event**Immigration & Refugee Law dinner**

The ADLSI Immigration and Refugee Law Committee is pleased to be again holding its annual dinner with the Minister of Immigration, the Hon Michael Woodhouse.

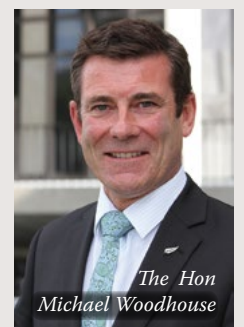
Immigration lawyers, licensed advisers and other senior figures in the immigration sector are invited to this valuable opportunity to meet and build rapport in a convivial setting.

The evening will include pre-dinner drinks and a three course dinner, plus a short address from the Minister.

Date: Monday 5 September 2016
Timing: 7.00pm arrival and drinks, 7.30pm dinner
Dress code: Business attire
Venue: Northern Club, 19 Princes Street, Auckland
Tickets: \$83.00 + GST (\$95.45 incl GST) for ADLSI members and the judiciary;
 \$95.00 + GST (\$109.25 incl GST) for non-members

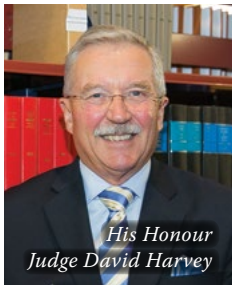
Spaces are limited so register before Wednesday 31 August 2016 to secure your space, subject to availability.

To register and pay for this event online, please visit www.adls.org.nz; alternatively, contact adls.events@adls.org.nz or (09) 303 5287. ADLSI’s standard cancellation policy applies for this event.



The Hon Michael Woodhouse

Prosecutions under the HDC Act



By Judge David Harvey

In August 2012, the Law Commission released a Ministerial Briefing Paper addressing harmful digital communications and the adequacy of sanctions

and remedies, entitled “Harmful Digital Communications: The adequacy of the current sanctions and remedies”. The Commission observed that the criminal law surrounding communications harms had focussed upon communications that invoke fears of physical consequences to persons or property or those which are obscene and harmful to children. The law had not concerned itself significantly with emotional harm although there were some developments in that regard.

In the paper, the Commission recommended the introduction of a new offence which targeted digital communications which were “grossly offensive or of an indecent obscene or menacing character” and which caused harm. It considered that there was justification for a tailored offence which would provide a primary mechanism to address egregious communications harms at the high end of the scale. During its investigation, the Commission noted an article that expressed concern that laws that are overly expansive and catch communications that do not deserve the heavy penalties imposed by the criminal law, suggesting that such laws should be tailored to deal with the most serious and deliberate cases of harassment or bullying, and noting the chilling effect of broadly worded criminal offences (see Jacob H. Rowbottom “To Rant, Vent and Converse: Protecting Low Level Digital Speech” (2012) 71 CLJ 355). On that matter, the Commission had this to say in its paper:

“We have been mindful of this caution and have been careful to put forward tailored amendments to our law that include suitably high thresholds so that only those communications that have caused serious harm come within their scope.”

In light of that, the Commission suggested that only the most serious and deliberate cases of harassment and bullying would come before the Court. Yet in the space of eleven months there have been 38 prosecutions, which has been something of a surprise. There are a number of possible reasons for this. One may be attributed to public awareness of the problem of cyberbullying and the publicity and controversy that attended upon the passage of the *Harmful Digital Communications Act 2015* (HDC Act). Another may be the nature of the offence and the difference between that proposed by the draft Bill prepared by the Commission and the offence as it was finally enacted in section 22. It is this author's view that the offence originally conceived by the Commission was far more restrictive in its scope than section 22 as enacted.

A third reason may lie in the fact that the nature of digital communications that have been the subject of a prosecution are more prevalent, far more vituperative and far more serious than was anticipated by the Law Commission.

This article will compare the Law Commission's proposal for an offence with the provisions of section 22 as enacted and then considers the cases that have come before the Court and to which guilty pleas have been entered, the content of some of the communications the subject of prosecutions and closes with some tentative conclusions.

The Law Commission proposal and section 22

The Law Commission proposed that an offence be added to the *Summary Offences Act 1981*. The language of the proposed section read as follows:

“21A *Causing harm by means of a communications device*

- (1) *A person (person A) commits an offence if person A sends or causes to be sent to another person (person B) by means of an communications device a message or other matters that is*
 - a. *Grossly offensive; or*
 - b. *Of an indecent, obscene, or menacing character; or*
 - c. *Knowingly false*
- (2) *The prosecution must establish that –*
 - a. *Person A either –*
 - i. *Intended to cause person B substantial emotional distress; or*
 - ii. *Knew that the message or other matter would cause person B substantial emotional distress; and*
 - b. *The message or other matter is one that would cause substantial emotional distress to someone in person B's position; and*
 - c. *Person B in fact saw the message or other matter in any electronic media.*
- (3) *It is not necessary for the prosecution to establish that the message or other matter was directed specifically at person B.*
- (4) *In determining whether a message or other matter is grossly offensive, the court may take into account any factors it considers relevant, including –*
 - a. *The extremity of the language used*
 - b. *The age and characteristics of the victim*
 - c. *Whether the message or other matter was anonymous*
 - d. *Whether the message or other matter was repeated*
 - e. *The extent of circulation of the message or other matter*
 - f. *Whether the message or other matter is true or false*
 - g. *The context in which the message or other matter appeared.*
- (5) *A person who commits an offence against this section is liable to imprisonment for a term not exceeding 3 months or a fine not exceeding \$2,000.*
- (6) *In this section communication device means a device that enables any message or other matter to be communicated electronically.”*

The type of offence created by section 22 was similar to that proposed by the Commission, but the way it was articulated was quite different

(for the full text of section 22 as enacted, see the New Zealand Legislation website www.legislation.govt.nz/act/public/2015/0063/latest/whole.html#DLM5711856). The first thing is that the message or other matter sent by means of a communications device has become a “digital communication” (meaning any form of electronic communication, including any text message, writing, photograph, picture, recording, or other matter that is communicated electronically). The act of communicating it is covered by the term “posts a digital communication” (meaning to transfer, send, post, publish, disseminate, or otherwise communicate by means of a digital communication any information, whether truthful or untruthful, about the victim, or an intimate visual recording of another individual (including attempts to do any of these things)).

The content of the communication in the Commission's draft was very specific. It had to be grossly offensive or of an indecent, obscene, or menacing character or knowingly false. In addition, it was necessary for there to be proof of an intention to cause substantial emotional distress, or an awareness that the message would cause substantial emotional distress. That was accompanied by a test that the message would cause substantial emotional distress to someone in the victim's position. Finally, there had to be proof that the person complaining actually saw the message in any electronic media.

The HDC Act, on the other hand, provides a content test based on harm rather than a strict categorisation of the nature of the content. The requirement of knowledge that the message would cause harm is not present, but there is a specific intention provided that the person intended to cause harm by posting a digital communication. There has to be proof of actual harm and a mixed objective subjective test that the posting of the communication would cause harm to an ordinary reasonable person in the position of the victim. However, there is no requirement that the victim actually see the digital communication, as was proposed by the Law Commission. Rather, section 22(4) defines the victim as the target of a posted digital communication. The reality is that most victims will be both the target and the recipient or viewer of the communication but the definition in section 22(4) does not make that clear. It is possible that a victim might not see the communication but be the subject of the communication and be told about its existence by a third party.

What amounts to harm?

The issue of distress is taken up by the definition of harm. As will be recalled, the element of substantial emotional distress was an element that had to be proven pursuant to subclause (2) of the Commission's draft. “Harm” is defined in the HDC Act as “serious emotional distress”. This may be similar to “substantial emotional distress” but what is missing is the nature and quality of the communication. All that is required is that a communication, virtually of any material, may be harmful if it causes serious emotional distress.

Continued on page 9

Continued from page 8

The specific content of the message is not factored in to the equation. There are certain limiting factors, such as the mixed objective/subjective test in section 22(1)(b). In addition, the court may take into account any factors it considers relevant including seven criteria that were articulated as a test to determine whether a communication was grossly offensive. These criteria are repeated verbatim in section 22(2)(a)-(g).

In its proposed section, the Commission had a two stage test. The first stage examined the nature and content of the communication. Did it fulfil the three criteria in (1)(a)-(c)? Seven factors were set out that might assist in considering the nature and content of the communication. Then once the quality or content threshold had been established the enquiry went on to consider the second stage – the issue of substantial emotional distress. The HDC Act, however, conflates the quality/content issue with that of serious emotional distress, and the only aspects of quality of content involve consideration of the extremity of language, truth or falsity and context. But rather than adopt the careful balancing of interests, and in particular that of the freedom of expression as the Commission did, the dominant element is harm or serious emotional distress.

What is needed to establish harm?

In its paper, the Commission used the general term “harmful digital communication” to cover a spectrum of behaviours involving the use of digital technology to intentionally threaten, humiliate, denigrate, harass, stigmatise or otherwise cause harm to another person. Cyber-bullying, on the other hand, was reserved for abuses that occurred within the context of adolescent peer relationships. The Commission gave consideration to the issue of emotional harm, observing that the criminal law was primarily concerned with the creation of fear of a particular sort – physical damage to person or property. There has to be a relationship between the potential of physical damage and the distress or mental harm that accompanies it. It went on to observe that the fear which anticipates physical harm is not physical harm itself. It is a state of mind which may or may not be more severe than other kinds of distress such as humiliation or the fear of a verbal attack. Both were forms of emotional harm. Both should be viewed equally.

In addition, it was observed that the distinction between physical and emotional harm had broken down over the years. In *R v Ireland* [1998] AC 147 (HL), it was observed (at 156) by Lord Steyn that “the civil law has for a long time taken account of the fact that there is no rigid distinction between body and mind.” (The tort of the intentional infliction of mental shock or distress was recognised as long ago as 1897 in the case of *Wilkinson v Downton* [1987] 2 QB 57.) The example was given of the tort of invasion of privacy which addresses an intangible harm.

Breach of privacy recognises that a form of damage may be in the form of significant humiliation, loss of dignity or injury to feelings. Distress is a basis for the making of a restraining order under the *Harassment Act*. To disturb, annoy or irritate a person by the use of a telephone device is an offence against

the *Telecommunications Act*. It should also be noted that injured feelings may find redress in aggravated damages and in contract damages may lie for emotional distress. Thus it can be seen that the law is no stranger to the concept of the causation of emotional harm as warranting the availability of a remedy.

The statistics – dates of offending and guilty plea cases

Between the time the offence section commenced (3 July 2015) until 17 June 2016, there had been 38 charges laid. Of those charged, 14 pleaded guilty, 16 entered not guilty pleas and, as at 17 June 2016, eight of those charged entered no plea. Of the 38 charged, 37 were male and one was female. One person charged was 15 and was dealt with in the Youth Court. The ages of the adults charged ranged from 17 to 61. 20 charges originated in the South Island, the balance in the North. The greatest number of charges – four – were laid in the Dunedin District Court. Of all the 14 cases where guilty pleas were entered, all but three had been sentenced as at the date of writing. Those awaiting sentence committed their offences on 20 January 2016, 8 March 2016 and 2 April 2016. This has meant a delay before disposal of up to seven months in the longest outstanding case.

The cases where pleas of guilty were entered have provided some interesting and disturbing examples of the quality of the communication that has been the subject of the charge. This tends to suggest that the use of digital communications systems for the purposes of abuse, harassment and extreme embarrassment is far more widespread than the Commission anticipated, and suggests that in fact the legislative recasting of the offence of causing harm by posting a digital communication has not set too low a threshold. Most of the cases to which guilty pleas have been entered have involved communication by way of Facebook, are within the context of a broken relationship and the messages are of a threatening or revengeful nature. Some involve the distribution of intimate images. Only one case involved communications to a victim where there appeared to be no relationship and that the communications were gratuitously abusive and insulting. Some involve the distribution of intimate images with a commentary. Three cases involved the use of text messaging and one involved the use of Instagram.

Examples of harmful communications

The following are representative examples of the communications that were the subject of prosecutions to which guilty pleas were entered. In one case (*Police v Lang* [2016] NZDC 11488), a communication was sent to a shared email account accessible by the victim’s workmates, involving 11 photographs of the victim in various states of undress, including three photos of the victim’s exposed breasts and four photos of the victim in her underwear.

Another case (*Police v Williams* (District Court, Tauranga CRI 2015-070-004137)) involved photographs which were posted on Facebook. One photograph showed the victim naked with only an open dressing gown on with her breasts and groin area clearly visible. Another photograph was of the victim in a seated position with no top on and her breasts could clearly be seen. Demeaning and insulting messages were

also posted reading: “Well played I know you’re a player, love having sex from all the guys”; “By the way you’re (sic) life is a living hell, I rather see you in jail where you belong whore slut”; “Hey slut have a look at my timeline you’re on there naked; and “Yum nice sexy slut look at that body”.

The victim said posts caused her serious harm in that they embarrassed her because all of her friends and family could see the photos and the comments. She was too scared to go outside in the event the defendant took further photographs of her. The defendant said he posted the images and photographs on Facebook as he was hurting and he wanted revenge and to cause the victim harm for hurting him. He claimed that the victim knew he had taken those naked photographs however he knew that he should not have posted them on Facebook.

A further case (*Police v Black* (District Court, Greymouth CRI 20-16-018-000021)) involved the use of Facebook private chat. The content of the communications was in the form of degrading and obscene sexual remarks. There were some twenty threatening messages included telling the victim to slit her throat, that she was a bad mother and that she was a waste of space. The victim stated that the communications made her feel worthless and ugly. For his part, the defendant stated that the victim said several similar things to him in person and that he wanted to get back at her by making her feel bad.

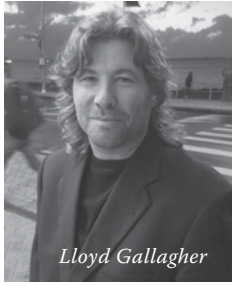
In another case (*Police v Bisschop* [2015] NZDC 24183) which involved the use of Instagram, the communication was in the form of a number of hashtags and phrases which together amounted to threats of damage to property and personal injury. The message read, “The joys of an crazy ex #brokenwindow #kickedindoor #accordeuro #frosty #glass #bitchneedsabullet #crazyexgirlfriend #lowblow #poorcar #handaaccord #wintersmorning #paybackwillcome @[victim’s Instagram address]” This was followed by an icon (cartoon picture) of a firearm. This caused the victim to become fearful for her safety, especially because she and her young son lived alone.

The final example (*Police v Kelly* (District Court Invercargill CRI 2016-025-000506)) involved a posting of photographs on Facebook with a commentary. The photos were of an intimate nature and depicted the victim naked in a shower. The comments read – “WHY THE F*** DID I DATE YOU LOL” - “LIKE Y DID I DATE THIS FAT SACK OF S**T CHEATING F***IN HOE BAG” - “NEEDS A SHAVE BOYS” - “THAT FAT ROLL.”

It is quite clear that social media is used for the purposes of revenge or exacting some form of retribution. Many of the cases under study have been in the context of failed relationships and the misuse of intimate images acquired either consensually or otherwise in the course of those relationships. Quite clearly the objective is to hurt and embarrass within the context of public fora such as Facebook. It is also clear that the use of such images and the language employed in the examples given is not just to provide an irritant but to seriously upset the victims in front of friends, family or the public. There can be little doubt of the intention to cause harm within the meaning of the HDC Act. In addition the language used and the images displayed breach

Continued on page 16

Electronic vs digital signatures – the same thing?



By Lloyd Gallagher,
Director/Arbitrator/
Mediator, Gallagher
& Co Consultants Ltd

The increase of electronic transactions has driven the need for clear confirmation of engagement.

From signing for courier deliveries to general form contracts, electronic signatures have become the normal practice for business. But are these legal? Can they properly bind parties? And who will be liable when things go wrong?

Under the common law, signatures have been recognised as a wide variety of marks or symbols, whether written, printed or stamped onto paper documents. While there are some documents (such as wills, affidavits, statutory declarations, negotiable instruments, bills of lading and certain medical certificates) that are excluded from using any form of electronic or digital signature (see the Schedule to the *Electronic Transactions Act 2002* for full details), for many other general form contract and simple transactions, electronic and digital signatures are well-placed to be used. And, while many New Zealand statutes require signatures, there is currently no general statutory definition of a “signature” under New Zealand law.

This article will address some of the issues with electronic signatures, how they compare to digital signatures, issues around security and encryption, and with which party/parties liability may fall if things go wrong. Whether or not relief might be available under contract law, tort, breach of confidence or consumer law is also considered.

What is an “electronic signature”?

“Electronic signatures” and “digital signatures” are two terms that are commonly used to mean the same thing. Even within the security industry, marketing people often tend to use the two terms interchangeably. However, this is incorrect as they have very different meanings, so at the outset, let us clarify the distinctions between electronic signatures and digital signatures.

An “electronic signature” is any signature that is in electronic form, as opposed to paper-based ink signatures – for example, a scanned image of your ink signature, a mouse squiggle on a screen or a hand-signature created on a tablet using your finger or stylus, a signature at the bottom of your email, a typed name, a biometric hand-signature signed on a specialist signing hardware device, a video signature, a voice signature, a click in an “I Agree” checkbox, or any other form of electronic medium to indicate acceptance of an agreement.



The *Electronic Transactions Act 2002* (ETA) is the key piece of legislation in New Zealand in this area and takes the form of overarching legislation and applies to all aspects of private and public sector activity, not just to commercial activities. It enacts a general rule that legislation currently requiring dealings to take place in paper format, unless expressly excluded from the scope of the ETA, will also be able to take place electronically if all the parties consent (sections 14 and 16). It is drafted in a “technology neutral” tense, making it well-placed to keep pace with the speed of changing technology systems.

Electronic signatures are defined within the ETA as meaning “in relation to information in electronic form ... a method used to identify a person and to indicate that person’s approval of that information” (section 5). The list is potentially endless and the main point to remember is that an electronic signature is any “mark” made by the person to confirm their approval of the document or transaction. Section 22 stipulates that the legal requirement for a signature will be satisfied by an electronic signature if it:

- adequately identifies the signatory and the signatory’s approval of the relevant information;
- is as reliable as is appropriate given the purpose for which and the circumstances in which the signature is required; and
- in the case of a signature on information that is required to be given to a person, that person consents to receiving the electronic signature.

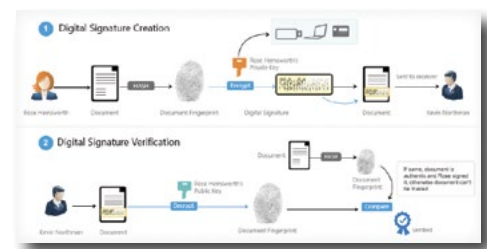
The benefits of this approach are the lack of restrictions placed on market-driven developments, the regulation of electronic signature technologies and the continuing application of the legislation despite any of these developments. The disadvantages are the continuing uncertainty as to the authentication of signatures and the varying degrees of reliability required for different classes of transactions.

Section 24 sets out some formalities required when an electronic signature is used – it must be linked to the signatory (or other authorised person) and to no other person, it must be verified, submitted by a known author (who cannot deny having affirmed the document or information signed), and the document or information must be able to be verified as unaltered in transit (or in other words, any alteration to the document or information must be detectable). Where there is a requirement that a signature or seal be witnessed, this is addressed in section 23, which provides that this can be met (apart from the exceptions set out in the Schedule) by a witness’s electronic signature if it complies with certain listed criteria (see section 22) and the person receiving the electronic signature has consented to receiving it in electronic form.

What is a “digital signature”?

A “digital signature” is a subset of electronic

signatures, as they are also in electronic form. However, digital signatures go much further by providing security and trust services in the signature delivery. When activating a digital signature, the signer is verified through authentication, the data is maintained on an integrity server for cross-checking and the signature is secured by encryption to prevent repudiation and modification in transit. Accordingly, a digital signature can be considered an electronic signature, but an electronic signature cannot be considered a digital signature. This is an important distinction when issues of validity and repudiation come into play.



Electronic vs digital – pros and cons

A number of useful guidelines on electronic signatures have begun to appear overseas (including in the UK) to assist counsel. One example can be found in the United Nations Model Law on Electronic Commerce, which has been used by our Law Commission in its examination of electronic signatures (see the “Further reading” section at the end of this article). The tables opposite provide a quick summary of the pros and cons for each signature type.

Security ... and what happens when encryption fails?

In general, there are two levels of security provided in today’s encrypted digital transmission technology – digital transmissions (bits and bytes sent intermittently and reassembled on receipt), and physical encryption processes added to the digital transmission using algorithms. I say “today’s”, because the technology is moving so fast that new technologies may be present tomorrow.

To encrypt a communication, a party can use software or hardware that incorporates an algorithm. Algorithms are complex mathematical functions for converting plain text into cypher-text and back again. A communication in binary form and a key (this is often a passphrase) are plugged into the encryption algorithm, the software or hardware executes the algorithm and the result is an encrypted communication. A unique key results in cypher-text which is unique in character. Where a different key is used, or if a different communication was the source, the cypher-text would be different.

While strong cryptography is very powerful when it is done right, it is not a panacea. Focussing on cryptographic algorithms while ignoring other aspects of security is like

Continued on page 11

Electronic signatures**Pros**

- Provides better user experience as can reflect normal ink signatures by using graphical images which users easily identify with.

Cons

- Can be easily copied or forged from one document to another.
- Document can be changed easily after signing without detection.
- No verification of who actually signed the document, so signatures can be repudiated.
- No automatic equivalence to handwritten signatures in most jurisdictions.

Digital signatures**Pros**

- Signed document cannot be changed (even a little) without detection.
- Who signed the document can be determined with a high degree of trust.
- Signers cannot repudiate their signatures.
- Some overseas cases have accorded digital signatures the same validity as handwritten signatures.

Cons

- Based on cryptographic codes and not as easily associated with normal ink signatures for users.
- Require multiple steps by users in the process to finalise the signature – they must log in to server, load document, sign using signature system and send to other side for authentication.

defending your house, not by building a fence around it, but by putting an immense stake into the ground and hoping that the adversary runs right into it. Smart attackers will just go around the algorithms. There are many attack strategies that can be successful and attackers exploit errors in design, errors in implementation and errors in installation without mercy, potentially opening the way for liability.

Dealing with multiple parties

Before dealing with possible liabilities, it is worth looking at the various parties usually associated with encryption processes. These may include:

- an encryption expert (who creates the encryption software), a security firm (employed to implement that software as part of a business security system);
- internet users (who may be expected to demonstrate certain levels of care in preserving confidentiality in internal and external transactions);
- the online service providers (who provide the facilities for transporting the encrypted information between parties); and
- the clients whose information or copyrightable material is the subject of the encryption process.

Issues in contract

Contracts affirm the right of parties to decide freely who bears the brunt of liability if the technology fails, subject to qualifications such as inequality of bargaining power and monopoly contracting. Ideally, counsel should address these issues during drafting, as problems are likely to arise where liability is left open, leading to time and money costs in resolving disputes. It is also important to carefully consider terms used, as providers in this area often have greater

technical knowledge than counsel and clients. The provision of encryption services may be an express term of the online service provider's contracts, and sometimes the service provider is simply a reseller and excludes liability to the third party or encryption expert. Encryption terms may also be open-ended and not address the standard of the encryption services. Accordingly, obtaining information from a technical professional or consultant is always good practice.

Determining whether a particular custom or usage is a term of a contract can also be difficult. It is suggested that counsel adopt the following good practice principles when reviewing a contract term:

- it must be so well known that the parties must have known of it and have intended it to form part of the contract (*Woods v N J Ellingham & Co Ltd* [1977] 1 NZLR 218; see also *Black v Falconer* [1916] GLR 627);
- it must be certain (*Woods v N J Ellingham & Co Ltd* [1977] 1 NZLR 218);
- it must be reasonable (*H F Moss Ltd v Andersen* (1914) 33 NZLR 606);
- it must be proved by clear and convincing evidence (*Woods v N J Ellingham & Co Ltd* [1977] 1 NZLR 218); and
- it must not be contrary to an express term of the contract (*Fairbanks, Lavender & Son v Low Bros* (1893) 12 NZLR 302).

Despite good drafting, the courts may still imply terms for encryption standards as encryption technology develops and becomes more common. Courts may also begin to imply terms as to the standard of the technology where needed to give efficacy to the contract. However, service providers holding a passive role are unlikely to be held to such standards

based on current approaches – to date, the courts have been reluctant to imply such terms simply to protect parties from a bad bargain. Furthermore, advances in encryption mean that any standard of acceptable technology will always be changing, making it difficult for a court to determine if a provider has fallen below such a standard.

If counsel is dealing with an existing contract which does not set out as encryption standard, all is not lost – courts may imply such a term if the party can show that the custom for the type of service provided includes the encryption service to a particular standard, or if the party alleging failure can show that such a standard is required to give efficacy to the contract (subject to it being shown that the failing party should have known that such a standard was necessary for the efficacy of the contract and that the contract would be ineffective without it, that the standard is reasonable, equitable, obvious, non-contradictory of any express term of the contract and capable of clear expression). This, however, is fraught with difficulties and counsel would be best to deal with such requirements within an express term.

Issues in tort

Where a service provider delivers encryption services of a poor or inferior nature that fails to adequately encrypt (“adequate” being subject to the defined terms of the contract or generally accepted standards), the tort of negligence may provide a remedy. It is well understood that the categories of negligence are never closed, but to bring an action home the alleging party will need to prove that the provider owes a duty of care to the plaintiff. This can be particularly difficult in the case of third party resellers and care should be taken to bring the action against the correct defendant. Consider: does an online service provider owe a duty of care to its customer to engage a reasonably skilled encryption expert? Does the encryption expert owe a duty of care to the online service provider to create an adequately secure system?

Situations falling outside a recognised duty of care may still come within the prescribed tests in *Anns v Merton London Borough Council* [1978] AC 728. Based on the first limb of that test, it is possible for an online service provider of encrypted transmissions with a sufficiently proximate relationship to its customer to foresee that any failure in those services could cause its customer damage. If this can be shown, a court may conclude the provider does owe a prima facie duty of care (provided that encryption was an expectation of the arrangement). This would be in line with cases where persons in professions and trades have been held to owe a duty of care in providing services. Examples can be seen where workers operating machinery in the vicinity of electric cables that supply power to a factory have been held to owe a duty to exercise reasonable care to avoid damaging the electric cables and interrupting the power supply to the factory (*SCM (United Kingdom) Ltd v W J Whittall and Son Ltd* [1971] 1 QB 337). Similarly, the provider of the encryption technology and the security firm may also owe a duty of care to the online service provider.

However, while the law of negligence in New

+ ADLSI Committees

Committee membership applications 2016/2018

ADLSI has a proud history of contributing to the law through its active member Committees programme.

Sixteen ADLSI Committees operate at present, comprised of volunteers who carry out a wide range of activities in their specialist areas. Committee appointments will be two year terms aligned with the ADLSI financial year, from October 2016 to September 2018.

Applications for membership on the below-listed Committees for 2016/2018 are now open.* ADLSI encourages applications from members throughout New Zealand – attendance at meetings can be accomplished not only by physically attending the meetings, but also by remote participation via phone and video conferencing.

Successful Committee applicants appointed by the ADLSI Council will be notified in mid-late September, with the first Committee meetings taking place in October.

New Committee members, as well as existing Committee members wishing to remain on their

current Committee, should apply online at <http://www.adls.org.nz/for-the-profession/201618-committees-application/> by **5pm, Monday 5 September 2016.**

(*Please note that Committee appointments cannot be confirmed unless the applicant is a

member of the ADLSI and this membership must be maintained during the course of the Committee appointment.)

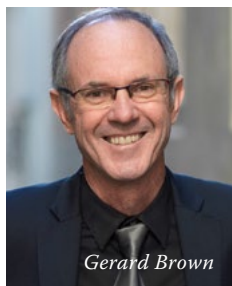
For further information or assistance, please contact Jodi Libbey on (09) 306 5744 or by email at Jodi.Libbey@adls.org.nz.

ADLSI has Committees in the following key areas – which might be the one for you?

- Civil Litigation
- Commercial Law
- Continuing Professional Development
- Courthouse Liaison
- Criminal Law
- Documents & Precedents
- Employment Law
- Environment & Resource Management Law
- Family Law
- Immigration & Refugee Law
- Health and Safety Law
- Members Special Fund
- Mental Health & Disability Law
- Property Disputes
- Property Law
- Technology & Law

+ Law and technology, member benefits

How an Auckland law firm reached for the Cloud



“We sensed that the ‘Cloud’ was the future in IT but we didn’t really understand it. However, we did know that our server was limiting us in terms of time and capacity. That’s really where it all started,” says Gerard

Brown, founding partner at Brown Partners – a boutique corporate law firm established in 2008 and now with seven lawyers and two support staff, based in Auckland’s Shortland Street.

Since inception, the firm had a typical IT set-up, which involved buying its own software licences and a server on site which was maintained by an external IT consultant. Mr Brown knew that the time and cost involved in patching up the bugs, plus the downtime involved to fix things, was costing the firm.

“We had meetings with various IT consultants to understand how we could be doing things better, but nothing really stood out as being the way of the future. Then I spoke with a former colleague and now partner of another boutique law firm and he recommended Appserv. That was really the turning point for us and we haven’t looked back.”

Appserv specialises in providing an end-to-end IT solution for law firms. Recently acquired by Spark, they are a pioneer in NZ Cloud IT technology services.

“I didn’t really understand the Cloud but I did understand we needed to change the way we did things and I wanted to modernise the way the firm approached IT. Our server was out of date and we were spending too much time patching up issues, getting the IT guys in and generally worrying about the equipment in the office and what may or may not happen to it – plus all the risks around data security and back-ups. Now we don’t have any of those issues.

“They really impressed me with their professionalism and understanding of what a legal firm needs from an IT system to operate at the highest level. They spoke my language and during the process I got a great understanding of how Cloud computing works.”

Appserv now houses all of Brown Partners’ IT environment, including data, software applications and internet, in its world-class data centres based in Auckland, and delivers it to the law firm’s desktop via secure connections. Everything is backed up with 24 hour, seven day service and even the firm’s telephony is run over the IT network. Now Brown Partners does not need to worry about software licensing, IT consultants, server issues or even computer costs.

“Basically, everything is delivered at a fixed monthly cost. Our computers don’t have to store anything so we can slim down on the specs when we have to replace them and I get access to the same desktop whether I am at work or home on any device. It’s taken a whole layer of administration and uncertainty out of the firm and everything just works.”

Appserv works with law firms to help them understand how the Cloud service works and produce very detailed proposals that show every facet of the process and system.

“The process was flawless. We were fine with the install costs and I was pleasantly surprised at the monthly price. We’ve got our entire communications and IT package wrapped up for us and we believe we are significantly better off doing it this way than doing it by ourselves.

“As lawyers, we can be quite critical but I don’t have a single issue with how this all played out for us, the outcome is exactly what was promised. This is easily one of the best decisions we’ve made as a business and I would recommend that any law firm that manages its own IT should consider talking to Appserv.”

Appserv is a supplier in the ADLSI Member Benefits Programme. To find out more about how Appserv could benefit your practice, call Appserv on 0800 85 85 66 or email info@appserv.co.nz.



publishers and distributors to let them use the token for a certain amount of time. The smart contract would include terms such as licensing fees, royalties. The contract may include a term which requires that the book publisher or distributor guarantee a certain amount of sales. If the publisher or distributor is unable to meet those obligations, then the digital token gets automatically revoked and the publisher or distributor no longer has the right to print the book or distribute the film. All of this would be executed automatically by the programme, and controlled by the parties themselves.

Block chain technology has the potential to solve problems faced by copyright owners, publishers, RROs and users to enable a more accurate record of use, and for a more granular management of

access to copyright content and costs by large institutions.

Further reading:

- *Blockchain Technology Glossary*: <http://www.blockchaintechnologies.com/blockchain-glossary>.
- Ruari Elkington, "Copyrights and Copywrongs: Reforming Educational Film Rights" <https://theconversation.com/copyrights-and-copywrongs-reforming-educational-film-rights-19392>.
- *Ethereum*: <http://www.ethereum.nz/>.
- Jeff Herbert, Alan Litchfield, "A Novel Method for Decentralised Peer-to-Peer Software License Validation Using Cryptocurrency Blockchain Technology," *Proceedings of the 38th Australasian Computer Science Conference (ACSC 2015), Sydney Australia, 27-30 January 2015 from*

<http://crpit.com/confpapers/CRPITV159Herbert.pdf>.

- *International Federation of Reproduction Rights Organisations (IFRRO) Relationship between Reproduction Rights Organisations*: <http://www.ifrro.org/node/26>.
- Brian Karlovsky, "Australian Writers' Guild launches multi-million dollar Federal Court action from Vincent O'Donnell" <http://if.com.au/2016/03/06/article/Australian-Writers-Guild-launches-multi-million-dollar-Federal-Court-action/TJFCAJNOO.html>.
- Jonathon Wolfe, "A Guide to Blockchain & its Potential Role in the Future of IP" <http://www.wrays.com.au/insights/news/a-guide-to-blockchain-and-its-potential-role-in-the-future-of-ip/>.

Continued from page 11, "Electronic signatures and digital signatures: aren't they the same?"

Zealand is wide enough to impose a duty of care on an encryption expert, a security firm or an online service provider, policy reasons may limit the boundaries of tortious liability and the class of persons to whom the duty is owed, including seriousness of harm (as encryption failure is likely to be purely financial, any duty of care may be reduced), opening of the floodgates, and the existence of other alternatives for self-protection. In addition, there are questions of what constitutes adequate encryption. As mentioned earlier, standards are constantly changing, making it hard for the law to keep pace. Counsel formulating a negligence claim will similarly need to consider engaging experts to assist in explaining existing standards.

Confidentiality

Confidentiality poses a greater level of complexity when considering a claim for loss or harm. The Law Commission has acknowledged that the law for breach of confidence involving electronic transmission is uncertain in New Zealand. However, the Commission considers that a person who, without authority, intercepts a message containing confidential information may be subject to a duty of confidence.

The UK position illustrates that confidence cannot be maintained where the arena is public – see *BBC Enterprises v Hi-Tech Xtravision* [1989] 18 IPR 63. Here, the court held that the defendant's conduct in decoding an encrypted BBC broadcast did not constitute a breach of confidence. The judge considered that if an author chooses to place a coded message in a public medium, he cannot complain if members of the public decode his message. The judge continued, "If the content, once decoded, does not qualify for protection on confidentiality grounds, the law of confidentiality is not, in my judgment, of any relevance." If New Zealand courts follow *BBC v Hi-Tech* (which is not a binding authority here), a user of encryption is unlikely to succeed in a claim under breach of confidence.

To the author's mind, difficulties arise with

the UK approach as the internet, despite being a public place, has become the standard transmission mechanism for many day-to-day operations of government and businesses, and lower costs of internet connections mean that organisations place their trust in encryption methods. Perhaps that is the fallacy of the modern world, illustrating that where information requires enough security so as to be protected from interception, clients should be advised to use a dedicated form of connection rather than the internet.

Fair Trading Act 1986

An encryption expert, security firm or online service provider may be liable under several provisions of the *Fair Trading Act 1986* (FTA) for misleading and deceptive conduct and false representations.

For example, if a person in trade markets his or her encryption services as being of a certain level of security, and the statement is not true, then that person may be liable under the FTA for misleading and deceptive conduct (section 9) and false representations (section 13).

Consumer Guarantees Act 1993

An online service provider may be liable for the guarantees found in the *Consumer Guarantees Act 1993* (CGA). The courts have already accepted that computers fall within goods or services of a kind ordinarily acquired for personal, domestic or household use or consumption (CGA, section 2 – see *Rask v Kelly* (District Court, Dunedin, 941/96, 22 July 1997, Judge Everitt)).

As more and more consumers acquire computers and use encryption for their communications, encryption may also fall within the meaning of "services". An online service provider, under the definition of "supplier", may be liable for the guarantees in respect of services. Failure to provide adequate encryption services may constitute breaches of the guarantee as to reasonable care and skill and the guarantee as to fitness for particular purpose. These areas have

yet to be considered by the court, but counsel should be aware of them nonetheless.

Digital signatures trump the rest, but take care ...

As discussed above, the requirements for authentication and verification outlined in the ETA leave the general form of electronic signatures somewhat lacking. Such electronic signatures provide no path to authenticate the signer or the document, or to guarantee that the information is unaltered in transit. Further, as security is easily compromised, electronic signatures open clients to a range of potential liabilities that are better avoided.

Accordingly, digital signatures provide the only appropriate form for signing electronically that both conforms to the requirements of the ETA and is likely to be accepted by the courts.

Further reading:

- *Guidelines for counsel on the use of electronic signatures: 2016 Practice Note from the Law Society of England and Wales* <http://www.lawsociety.org.uk/support-services/advice/practice-notes/execution-of-a-document-using-an-electronic-signature/>; see also Law Commission "Electronic Commerce Part One: A Guide for the Legal and Business Community" NZLC Report 50, 1998, page 7.
- *Electronic Transactions Act 2002: Discussion Paper, Ministry of Economic Development, May 2000, at page 8.*
- *Encryption and algorithms: Smedinghoff, Online Law: The SPA's Legal Guide to Doing Business on the Internet, Software Publisher's Assoc, 1996, page 497; see also Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C, 2nd Edition, Wiley, New York, 1996, pages 223-225 and Bruce Schneier "Security Pitfalls in Cryptography" (1998) Counterpane Systems at 1.*
- *Encryption adequacy and standards: Lim "Liability Issues in Encryption Technology" (1998) 37 Computers & Law (Aus and NZ) 42, page 46.*
- *Confidentiality and breach of confidence: Law Commission "Electronic Commerce Part One: A Guide for the Legal and Business Community" NZLC Report 50, 1998, pages 3 and 61.*

To view all ADLSI CPD & register: www.adls.org.nz/cpd

Email us: cpd@adls.org.nz | Phone us: 09 303 5278

Featured CPD

Tuesday
30 August 2016
4pm – 6.15pm

2 CPD HOURS



Seminar



Live stream

Commercial Law Series: Commerce Act – Insights and Guidance – FINAL NOTICE

Competition law is not always intuitive. Potential and alleged breaches of the Commerce Act 1986 are frequently missed by clients – and sometimes by legal advisers. Particularly in the wake of legal developments in this area, lawyers need to be provide accurate, proactive advice and if necessary be able to advise a client about how to deal with a breach.

Learning Outcomes:

In respect of the Commerce Act:

- Become updated about legal developments: recent cases and the Commerce Commission's approach.
- Gain a better understanding of common issues and trends, like competitor dealings (including industry dealings), restraints of trade, online and multi-channel distribution, 'hub and spoke' cases, and merger control.
- Receive insights into and guidance for dealing with the regulator, including about its compliance materials and leniency programme.

Who should attend?

Commercial lawyers at all levels to upskill and/or for a refresher and general practitioners who do commercial work.

Presenters: **Andy Matthews**, Principal, Matthews Law; **Katie Rusbatch**, Competition Manager, Commerce Commission

Chair: **Geoff Hardy**, Partner, Martelli McKegg

Thursday
1 September 2016
5pm – 7.15pm

2 CPD HOURS



Seminar



Live stream

Common Criminal Procedures: Improving Your Practice – FINAL NOTICE

This seminar will cover four key criminal procedures: bail applications, discharges without conviction, sentencing indications and pleas/written submissions in mitigation. Attend this seminar to achieve better outcomes for your clients.

Learning Outcomes:

- Become updated on procedure for bail applications, including when to make an application and what to put before the court.
- Receive guidance on seeking discharges without conviction, including key case law in respect of relevant factors.
- Gain a better understanding of practice around sentencing indications, including whether to seek them.
- Gain insights into making more effective pleas/written submissions in mitigation, including key content to include and the structure most likely to assist the judge.

Who should attend?

Criminal lawyers seeking an update/refresher on these key areas of practice.

Presenters: **Phil Hamlin**, Barrister; **Michele Wilkinson-Smith**, Barrister

Chair: **His Honour Judge Earwaker**

Tuesday
6 September 2016
4pm – 6.15pm

2 CPD HOURS



Seminar



Live stream

Assisting First-Time Home Buyers: Exploring the Options

The agreements entered into by home buyers when purchasing their first property can take a variety of forms. Often, the complexities behind the financial and other arrangements are overlooked with real potential for unseen consequences arising later.

Learning Outcomes:

- Learn more about the options available to first-time home buyers including loans or gifts from parents and buying together with friends as well as what agreements will be needed to safeguard interests in each case.
- Understand better the way trusts can be used, either as a source of funds or as a vehicle of ownership.
- Gain insights into the potential for conflicts of interest that exist when advising the parties involved, the care that needs to be taken in respect of relationship property issues and how it is necessary for parents to balance the interests of all children.

Who should attend?

All property, trust and family lawyers as well as general practitioners who deal with work of this nature from time to time.

Presenters: **Bryce Town**, Partner, Morrison Kent; **Tammy McLeod**, Director, Davenport's Harbour Lawyers; **Stephanie Ambler**, Partner, Tompkins Wake

Chair: **Ian Jespersen**, Senior Associate, Burton Partners

Saturday
17 September
2016
9am – 5pm

6.75 CPD
HOURS



Intensive

Running an Effective Jury Trial – EARLY BIRD PRICING ENDS 27 AUGUST

Jury trials require a specific set of advocacy skills. Given the serious nature of cases heard in a jury trial setting, 'getting it wrong' can have significant implications for the accused – and for defence counsel. Aptitude in preparation and presentation is key.

Learning Outcomes:

See our website: www.adls.org.nz/cpd

Who should attend?

Although the focus of the intensive will be oriented towards those acting as defence counsel, the themes will be of practical use to all those commencing, or relatively inexperienced in, jury trial advocacy, as well as those more experienced who are seeking an update/refresher.

This intensive meets Ministry of Justice requirements as an equivalent course suggested for completion as part of an application for Criminal Provider Approval Level 2.

Presenters: **His Honour Judge Sharp**; **Paul Dacre QC**; **Marie Dyhrberg QC**; **Steve Bonnar QC**; **Simon Lance**, Barrister

Chair: **His Honour Judge Sharp**

CPD in Brief

Commercial Law Series: Franchising – The Legal Lifecycle – 1 CPD hr

Wednesday 31 August 2016, 12pm – 1pm

With franchising having ballooned in popularity as a method of business growth, so too have the number of franchise disputes. All too often complaints and disputes arise due to franchisees not realising what they have actually signed up for. This webinar will cover the lawyer's input at various stages of the 'franchise lifecycle'.

Presenters: **David Foster**, Director, Harris Tate (Tauranga); **Deirdre Watson**, Barrister



Interim Injunctions: Tipping the Balance – 2 CPD hrs

Thursday 8 September 2016, 4.30pm – 6.45pm

This seminar will offer practical guidance, for acting for plaintiffs and defendants alike in this important area. Topics include preliminary and strategic considerations; threshold issues; and the practicalities of making and defending an application, and gaining and enforcing an order.

Presenters: **Christine Meechan QC**; **Mark Colthart**, Barrister

Chair: **The Honourable Justice Courtney**



Ethics: Practical Guidance for Avoiding Common Pitfalls – 2 CPD hrs

Thursday 15 September 2016, 4pm – 6.15pm

Lawyers' conduct is regulated with an emphasis on consumer protection. Approximately 1600 complaints about lawyers are made annually and the need for lawyers to be vigilant in their professional dealings is greater than ever. This seminar will focus on the topics of conflicts of interest, dealings with clients' money, and duties of 'civility', and there will be a 'state of the nation' from the perspective of legal underwriters. This is a seminar which all lawyers should attend – for the sake of their practice and their personal and professional wellbeing.

Presenters: **Paul Collins**, Barrister, Shortland Chambers; **Bruce Galloway**, Consultant, Jones Young; **Philippa Fee**, Partner, Fee Langstone

Chair: **Paul Collins**, Barrister, Shortland Chambers



CPD On Demand

Dispute Resolution Clauses: Uses and Analysis – 1 CPD hr

Recent Supreme Court judgments have highlighted the importance of having knowledge of Dispute Resolution clauses when including them in commercial contracts. All too often, Dispute Resolution clauses become part of such agreements with little thought to content or whether they are really needed in the first place. In this On Demand webinar, learn how best to advise clients on what form, if any, Dispute Resolution clauses might take and gain insights into how best to tailor them to suit clients' needs.

Presenters: **Paul Cogswell**, Principal, Cogswell Law; **Nick Gillies**, Partner, Hesketh Henry



Privacy in the Digital Age: The Risks and Opportunities of New Technology – 1 CPD hr

Technology and social media are now inescapable aspects of modern life. They provide unique opportunities for individuals to interact with each other and for businesses to interact with consumers and to develop their brands. However, such opportunities raise inevitable legal questions. Privacy issues have, as a result, become increasingly complex. It is essential for lawyers to know how their clients' professional and personal privacy may be affected by technology and how to advise clients on avoiding privacy breaches or protecting them from unwanted attention. This On Demand webinar will assist.

Presenters: **Daimhin Warner**, Customer Governance & Privacy Manager, Sovereign Insurance; **Joe Edwards**, Senior Associate, Russell McVeagh



CPD Pricing

Delivery Method	Member Pricing	Non-Member Pricing
Webinar (1 hr)	\$75.00 + GST (= \$86.25 incl. GST)	\$95.00 + GST (= \$109.25 incl. GST)
Seminar (in person)	\$125.00 + GST (= \$143.75 incl. GST)	\$180.00 + GST (= \$207.00 incl. GST)
Seminar (live stream)	\$125.00 + GST (= \$143.75 incl. GST)	\$180.00 + GST (= \$207.00 incl. GST)
On Demand (1-hour recording)	\$85.00 + GST (= \$97.75 incl. GST)	\$110.00 + GST (= \$126.50 incl. GST)
On Demand (2-hour recording)	\$95.00 + GST (= \$109.25 incl. GST)	\$130.00 + GST (= \$149.50 incl. GST)

For group bookings for webinars & CPD On Demand, see the ADLSI website at: www.adls.org.nz/cpd/help-and-faqs/group-bookings/.

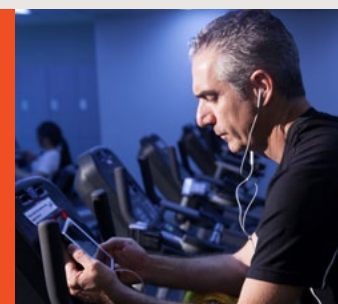


ADLSI members, non-member lawyers and law firms who have registered their Airpoints™ membership details with ADLSI can earn Airpoints Dollars™ on eligible ADLSI CPD purchases. Visit adls.org.nz for full details. *Terms and conditions apply.*

CPD On Demand

Compliant, convenient and cost effective.

Visit www.adls.org.nz/cpd for more information.



one or more of the communications principles.

Sentencing

Sentences for offences against section 22 have ranged from a discharge without conviction pursuant to section 106 of the *Sentencing Act* to a sentence of eleven months' imprisonment; other sentences of imprisonment have been for terms of three months and six months (see *Police v Tamihana* [2016] NZDC 6749, *Police v Lang* [2016] NZDC 11488 and *Police v Bust* [2016] NZDC 4391). In all the cases involving sentences of imprisonment there were other charges.

The case of *Police v Tamihana* received a detailed consideration of sentencing issues arising in cases involving a breach of section 22. There were other charges for breach of bail and two for intentional damage, but the lead offence was that against section 22 which the judge described as most serious. The offending arose within the context of a volatile relationship. However, the victim was not the partner of the defendant but her mother who had, on a number of occasions, tried to end the relationship. The defendant was aware of this. On 13 December, he sent a Facebook message to the victim with whom he had not previously communicated. The message included a video attachment with the comment, "What your daughter's really up to." The victim opened and played the video which the judge described as a sexual scene involving the defendant's partner and another. The partner was a consenting party to the making of the video. The victim was very upset, angry and sad to see her daughter being portrayed in this way. She felt feelings of despair and took the view that this was payback for her disapproval of the relationship. Every time she thought of the video it caused her further distress.

In his comments on the legislation itself, the judge made reference to the ease of dissemination of information on the Internet and what has been described as the "online disinhibition effect". The judge said:

"[W]e live in a world where it is very easy and certainly in a very cowardly way and impersonal third person way to communicate with others without fronting up yourself. The other problem of course is that in this day and age broad dissemination of such material is just at the touch of a button ..."

The judge stated that the actions of the defendant were designed to have the maximum possible impact upon the victim and that he

acted out of retributive malice in delivering a cowardly and sinister attack. He acknowledged that the HDC Act was new, and that there would probably be worse cases, but that he found it difficult to think of one. The principal objective of sentencing in this case was that of deterrence. The judge fixed a starting point of nine months' imprisonment with an uplift of three months for totality of offending and a further three for previous convictions. He then applied a 25% discount for the defendant's guilty plea. The deterrent message was emphasised by the rejection of a sentence of home detention.

In the case of *Police v Lang*, a sentence of three months' imprisonment was imposed, which was cumulative upon other sentences. The judge did not embark upon an analysis either of the facts of impact of the offending, primarily because the defendant was facing sentence on a number of other charges involving dishonesty. The victim of Lang's offending was his former partner. He sent an email to a shared email address at her place of employment to which other employees had access. Attached to the email were eleven photos of the victim in various states of undress including images of her exposed breasts and of her dressed in her underwear. The victim said that she did not consent to any of the photos being taken. He stated that his reasons for sending the images were that he wanted to return them to her and that he wanted closure for himself.

The case of *Police v Bust* involved a number of charges including cultivation of cannabis, possession of a methamphetamine pipe, driving whilst disqualified, and breaches of community work and release conditions. But the judge took the offence against the HDC Act as the lead offence. The sentence imposed had been the subject of an earlier sentence indication hearing. The communication in this case involved a text message to the victim over a drug debt and threatening the victim and his father in what the judge described as "a pretty serious way". The sentence of imprisonment of six months was imposed in accordance with the earlier sentence indication.

The defended cases

Of the charges to which pleas of "not guilty" have been entered, the dates of alleged offending tell an interesting story. As at the date of writing, none of the defended cases have been heard. By date of alleged offence the oldest took place on 19 August 2015. The most recent was alleged to

have occurred on 21 April 2016. Eleven cases arose in 2016 – the remaining five arose in 2015. Of those, there has been one disposal where a charge was withdrawn by leave (Alleged offence date 28 December 2015, Dunedin District Court CR 15044006509). Although trial by jury is available, none of the defendants have elected trial by jury and have chosen to be dealt with by a judge alone.

The delay in getting cases to hearing must be a matter of concern. Apart from the well-known stresses that are a part of having to relive offending during the course of giving evidence, the definition of harm as serious emotional distress means that victims will have to revisit this specific form of harm many months after the alleged offending took place. This can hardly be said to assist the recovery process. In addition, a specific purpose of the HDC Act is to provide victims of harmful digital communications with a quick and efficient means of redress. Although this probably refers primarily to the civil enforcement process it is my view that it must apply with equal force to the victims of section 22 offences. The language of the clause specifically refers to victim, and the word victim is used in section 22 and especially section 22(5). Given this specific purpose behind the legislation, the hearing of cases involving offending against section 22 should be accorded priority and should be expedited.

Conclusion

The "offence section" of the HDC Act has been in force for twelve months. It has attracted more prosecutions than the Commission envisaged. This paper concludes that there may have been an underestimate in the frequency and venom of online communications especially occurring in the context of failed relationships. The decision in *Police v Tamihana* sets some helpful guidelines for the factors that a Court should take into account when dealing with offenders charged with an offence against section 22. Deterrence is going to have to be a significant factor, especially given the ease with which the offence may be committed. It is suggested that, when one looks at the examples given in this paper from the cases where guilty pleas have been entered, the statutory threshold in section 22 has not been set too low. The content and effect upon the victims of the various communications must be of concern and warrants the involvement of the criminal law.



Investigating cybercrime

According to recent reports, each day there are over 108 reported cybercrime attacks in New Zealand.

"Cybercrime" is defined by the US Department of Justice as any illegal activity using a computer or storage device for commission/transmission of the activity.

This includes theft of important company intellectual property, as well as the misuse of company computer systems for purposes other than performing the employee's assigned tasks.

CheckIT© is a service provided by Computer Forensics NZ Ltd and is designed to provide information to assist you and your clients in making an informed decision as to whether further action such as litigation and a full, formal forensic

investigation is required.

It is a preliminary investigation, specifically for employers when they suspect an employee of either misusing company computer/device resources, or stealing valuable intellectual property.

We investigate the computer used by the employee (covertly if necessary) and provide a brief summary of the user's activities. It can be used if a key employee resigns, if supporting evidence of misconduct is required, if an employee is specifically suspected of wrongdoing, or as a random computer/device audit.

For more information or a quotation, call 0800 LOST FILES 0800 5678 34 or visit www.datarecovery.co.nz.

Special combo deal on internet and media law books

For a limited time, purchase Judge David Harvey's *internet.law.co.nz, Revised 4th Edition* plus *Burrows and Cheer, Media Law in New Zealand, 7th Edition* together from the ADLSI bookstore and receive a 20% discount off the regular price of both books (if you are a member of ADLSI), or a 10% discount (if you are not a member of ADLSI).



Published this year, the revised 4th edition of *internet.law.co.nz* contains new and updated material examining topics such as recent case law and legislation including the *Harmful Digital Communications Act*, the *Search and Surveillance Act* and amendments to the *Electronic Transactions Act*. It also looks at speech harms, cyber-bullying and harassment in social and other media, online defamation, content regulation and use of information technology in court.

In the 7th edition of *Media Law in New Zealand*, Ursula Cheer has comprehensively updated the text to reflect rapid changes in law since 2010, particularly with regards to defamation, privacy, breach of confidence, contempt and court reporting, official information and media complaints bodies. A new chapter on the New Zealand advertising standards regime has also been added.

Normally, these books together retail at \$300 plus GST, but by buying them together you can get them at the following special prices:

Special price for Non Members: \$270.00 plus GST (\$310.50 incl. GST)*

Special price for ADLSI Members: \$240.00 plus GST (\$276.00 incl. GST)*

(* + Postage and packaging. Offer available from Friday 26 August until Friday 30 September 2016 or while stocks last.)

To purchase this combo, please visit www.adls.org.nz; alternatively, contact the ADLSI bookstore by phone: (09) 306 5740, fax: (09) 306 5741 or email: thestore@adls.org.nz.

The Family Courts Association (Auckland)

invites you to their Celebration Dinner to honour the founding members of The Family Courts Association (Auckland) on **Monday 5 September 2016** commencing with drinks from 6pm

Venue:
Five Knots (Tamaki Yacht Club)
Tamaki Drive, Auckland

Cost: \$70.00

RSVP by **31 August 2016** to:
Alison Wilcox, Administrator
Email: admin@famcourtsassociation.org.nz
Mobile: 0274 879006



Personal Safety & Workplace Training

- Threat & Conflict Resolution
- Shop Theft
- Robbery Training
- Fraud Training

If it happened tomorrow, would you know what to do?

For more information visit our website: www.feelsafe.co.nz or call us on 09 827 0096.

Feel Safe is a specialist training provider, facilitated by Translegal.

WILL INQUIRIES LAW NEWS

The no-hassle way to source missing wills for **\$80.50 (GST Included)**

Email to: reception@adls.org.nz
Post to: Auckland District Law Society Inc.,
PO Box 58, Shortland Street, DX CP24001, Auckland 1140
Fax to: 09 309 3726
For enquiries phone: 09 303 5270

+ Wills

Please refer to deeds clerk. Please check your records and advise ADLSI if you hold a will or testamentary disposition for any of the following persons. If you do not reply within three weeks it will be assumed that you do not hold or have never held such a document.

Kyuhaeng BANG, Late of Metropolis Apartments, Courthouse Lane, Auckland, Aged 58 (Died 29'07'16)

Peter Geoffrey BELL, Late of 3/21 Deane Avenue, Titirangi, Auckland, Aged 69 (Died 24'07'16)

Lynette Carolyn HATT nee WEBSTER, Late of 34 Burn Street, Levin, Retired, Aged 69 (Died 15'07'16)

Roderick William McGAW, Late of 12 Titchener Street, New Lynn, Auckland, Aged 73 (Died 02'07'16)

Asari POI, Late of Auckland, Aged 83 (Died 11'08'16)

Michael Alan SCOTT, Late of Auckland, Machinist Joiner, Aged 59 (Died 31'07'16)

Jerry TOBIN, Late of 9 Friedlanders Road, Manurewa, Auckland, Road Worker, Aged 64 (Died 23'11'15)



Trusted practice management software for NZ lawyers

Easy to learn, easy to use. Save time and increase profits. That's what users say!

New: Document management & Internet banking. **Free** installation and training. Visit our website for testimonials from firms just like yours.

www.jpartner.co.nz enquiries@jpartner.co.nz 09 445 4476 JPartner Systems Ltd

GOODWIN YALLOP
ON DEMAND LITIGATION SUPPORT

Now you can outsource to the specialists:

- Discovery - processing, review, preparation of inspection sets
- Bundles and casebooks - electronic and print
- Strategic information management

ANGELA GOODWIN
021 749 208
angela@goodwinyallop.co.nz

SARAH YALLOP
021 721 727
sarah@goodwinyallop.co.nz

www.goodwinyallop.co.nz
Level 3, 43 High Street, Auckland



Working with, and creating law firms of the future

- Are you wanting to improve your office efficiencies?
- Do you need back up cover for when your trust accountant is away?
- Are you wanting to reduce your manual processes and increase overall productivity?

Our role is to help firms determine the best operating model for business support functions.

Change
Journey
Reward

info@pagezero.co.nz
(09) 470 2412
www.pagezero.co.nz

ROSS HOLMES
LAW • ASSET PROTECTION • TRUSTS

Head of Chinese Legal Division

We have an exciting opportunity in our Albany office for the head of our Chinese legal division. The position requires acting in the areas of business law, property law, and trusts to our Chinese client base. The position requires a self starter with excellent marketing skills who is capable of managing our Chinese legal team.

We are interested in people who:

- can write and speak fluent English, and Mandarin.
- are dedicated to giving our clients the best possible service.
- pay attention to detail and pride themselves on the quality of the advice they give.
- demonstrate strong interpersonal skills.
- have excellent organisational and marketing skills.
- display sound commercial judgement.
- have excellent computer skills.

In return we offer you:

- the chance to be part of a boutique business law, property law and trust firm;
- a professional environment;
- up to date technology;
- a competitive remuneration package.

If you would like to know more about these positions please call Michael Sheng on (09) 415 0099, visit our web site www.rossholmes.com or email us in strict confidence (including a transcript of your academic record) to: michaels@rossholmes.co.nz.

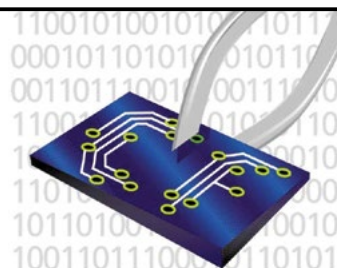
Ross Holmes Virtual Lawyers Limited

CLIENTS UNDER THREAT?

Stop just wondering about misuse of company IT resources, espionage, sabotage, malicious behaviour and theft of intellectual property.

FIND OUT CheckIT[©]

A preliminary investigation process, secure and covert if necessary for employers who need to be certain.



COMPUTER FORENSICS
Computer Forensics NZ Limited

Recovering data & fighting cybercrime since 1999

www.datarecovery.co.nz/checkit | Speak to us in confidence on 0800 5678 34

Tired of receiving High Court Registrar Minutes on estate drafting?

Estates drafting can be very complex and time-consuming.

We have 30 years' experience in this area and can remotely draft your probate / Letters of Administration, with or without will Annexed (including de bonis non) documents, and mail them to you, ready for printing and execution by your firm.

We also have experience in resealing and foreign wills.

Visit robinsandco.co.nz for further information or contact Denise Robins:

✉ denise@robinsandco.co.nz

] 09 373 9923 or 021 727 981

ROBINS
& CO

BARRISTERIAL OFFICE AVAILABLE

Durham West offices operates in refurbished premises in Queen Street (close to the District Court) sharing a floor (with separate areas) with Hussey & Co., a forensic and general accounting firm.

The offices are presently occupied by four legal firms/barristers and a personnel recruitment firm. A further lawyer/barrister is sought. The six tenants share a separate dedicated meeting room. If required, internet access, telephone, photocopier and other services are also available.

The room available is approximately 14m² (furnished or unfurnished) at a cost of \$260 per week plus overheads of approximately \$100 per month, plus GST, with no long term commitment required.

Photographs of the chambers can be viewed at www.hco.co.nz/gallery

For further details:

Contact: Shane Hussey

E: shane@hco.co.nz

T: 09 300 5481



It's the cloud based conveyancing software that's got everyone talking

conveyit Maestro is an automated cloud based conveyancing system designed by New Zealand Lawyers for New Zealand Lawyers, Professionals and Conveyancers



www.conveyit.co.nz



0508 33 22 88

DISCOVER AN EASIER WAY TO GROW YOUR BUSINESS

If you are running a law firm, the last thing you want is for IT to hold you back.

That's why spam protection, software upgrades, server maintenance and support issues are all a thing of the past with Appserv. If you want to add or remove users quickly, no problem – everything is priced per head per month. Need your data to be stored in New Zealand, no problem – it is.

Just ask Shortland Street Law firm, Brown & Partners:

"As lawyers we can be quite critical but I don't have a single issue with how this all played out for us, the outcome is exactly what was promised. This is easily one of the best decisions we've made as a business and I would recommend that any law firm that manages their own IT should consider talking to Appserv."

Appserv can help you navigate your law firm safely into the cloud and remove your IT headaches, allowing you to focus on core business. No drama, no fuss, it just works.



appserv.co.nz 0800 85 85 66

A company with





TRADITIONAL DRAFTING CHECKLIST:

- Is my definitions list complete?
- Is my writing crisp and easy to understand?
- Have I used all defined terms correctly?
- Are all the clause cross-references correct?
- Have I used consistent wording throughout?
- Have I cited the most up-to-date and relevant cases?
- Have my colleagues completed their parts?
- Have I attached the right documents?
- Are all my clauses numbered correctly?
- Have I completed any gaps I meant to come back to?
- Have I updated all information I needed to check?
- Is all my punctuation complete and clear?

MY DRAFTING CHECKLIST:

- Click 'Lexis Draft Pro'



Lexis® Draft Pro

DOES IT ALL FOR YOU

Lexis Draft Pro is part of the SmartOffice® Suite, giving you back more time to do what matters to you.

Contact our team today on **0800 800 986**.
Go to www.lexisnexis.co.nz/drafting for more information.