THIS WEEK'S ARTICLES

Issue 29
25 Aug 2017

ADLS
Connecting New Zealand Lawyers

LawNews

adls.org.nz

Technology & Law
SPECIAL EDITION

INTELLECTUAL PROPERTY AND TECHNOLOGY

Hidden advertising practices finally exposed

By Sophie Thoreau, Team Leader and Senior Associate, Baldwins Intellectual Property

Trade mark owners are becoming increasingly savvy in the way in which they use and protect their brands online and in social media. Most companies have guidelines and policies in place which govern their exposure online and will be quick to pick up on and address any usage that threatens to damage their reputation.

But what about usage that is unseen, hidden in website code or lurking behind the workings of a search engine? What damage could this really be doing to a trade mark's reputation? Should competitors be legitimately able to use others' brands to leverage their own success?

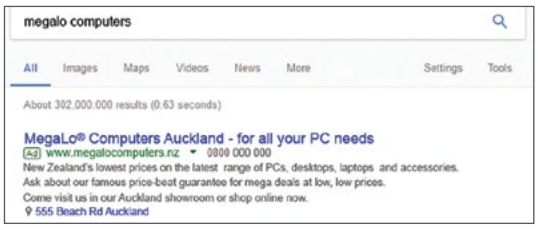
We update a decades-long battle that has raged almost since the inception of modern search engines.

Branded keywords, meta tags and "invisible" trade mark infringement

Unseen or "invisible trade mark" use typically falls into the category of branded keywords (such as Google's Adwords®) or website meta tags.

A branded keyword is a term or phrase used to search for a product or company via a search engine. The trade mark MEGALO® is an example of a branded keyword available on Google's Adwords® system, as follows:

Welcome to the fourth annual special "Technology & Law" edition, put together by ADLS' Technology & Law Committee.
We hope you enjoy it!



While branded keywords are mostly used by legitimate trade mark owners to direct their own customers to their website, they are increasingly being hijacked by competitors to divert traffic to another site, or increase their page ranking.

Google supports this practice in many jurisdictions, ostensibly to "offer useful alternatives to the goods or services of the trade mark proprietor".

Meta tags are hidden words or phrases that are embedded into a website's code. Their primary function is to talk to search engines to explain what a web page is about. Meta tags enable search engines to prioritise or rank web pages based on what they think a searcher

Continued on page 2

Hidden advertising practices finally exposed

Continued from page 1

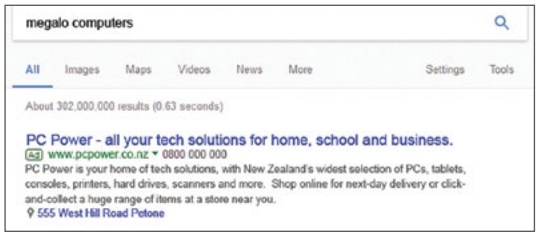
may be looking for.

Used properly, meta tags enable customers to quickly connect with the product or business they are looking for. Used strategically, meta tags can influence search engines to bring up competitors' websites and ultimately draw customers away from their intended destination.

Using third-party trade marks in branded keywords and meta tags

Courts have long battled with the notion of trade mark infringement where the trade marks in question are never seen by the customer. Under Australian and New Zealand law, in order for an act to amount to trade mark infringement, the allegedly infringing mark must be used in such a way as to be taken as use as a trade mark, by the relevant consumer.

Because branded keywords and meta tags are invisible to the end consumer (assuming the average consumer does not trawl through a website's source code), the position to date is that branded keywords and meta tags are not taken as trade marks, despite the fact that this is precisely how they are being used by the advertisers themselves. This means that the example below, in which "PC Power" could use its competitor's trade mark MEGALO® to advertise its own services, would currently be permitted:



***Accor* – a potential game changer?**

A recent Australian decision in *Accor Australia & New Zealand Hospitality Pty Ltd v Liv Pty Ltd* [2017] FACFC 56 suggests the Australian courts may be reconsidering their approach to invisible trade mark use, at least in relation to meta tags. In this case, the defendant was sued for trade mark infringement, including for the use of the plaintiff's trade mark HARBOUR LIGHTS, which it had inserted into its website as a meta tag. On appeal, the Federal Court of Australia ultimately held, divergent to previous case law, that although the meta tag containing the plaintiff's trade mark was not visible to the ordinary consumer, the use of the words "Harbour Lights Apartments" in that phrase was, effectively, use as a business name, thus operating as a badge of origin to distinguish Liv's services from others. This use was found to be use of a mark substantially identical with and deceptively similar to each of the registered trade marks in suit.

The *Accor* decision is an apparent sea-change following earlier Australian decisions such as *Complete Technology Integrations Ltd v Green Energy Management Solutions Pty Limited* [2011] FCA 1319, in which use of a third-party trade marks were clearly permitted. In that case, the judge held that although the meta tag usage diverted consumers away from the plaintiff to the defendant's webpage, ordinary internet users would quickly become aware of the diversion and thus would unlikely be confused.

Sophie Thoreau

> Advertisers may soon find themselves walking a fine line between hunting clicks and maintaining transparency.

The New Zealand position

New Zealand courts have been in line with the position in Australia, until now. In *Intercity Group (NZ) Limited v NakedBus NZ Limited* [2014] NZHC 124, the plaintiff failed to make a case for trade mark infringement in relation to Nakedbus' use of its registered trade mark, INTERCITY, in "invisible" branded keywords. The Court agreed with NakedBus' argument that there was no use of Intercity's trade mark in the course of trade because the keyword is invisible to consumers and therefore unlikely to be taken as a trade mark.

A later New Zealand decision, *Tasman Insulation New Zealand Limited v Knauf Insulation Limited* [2015] NZCA 602, recognised that use of a registered trade mark in a meta tag could be taken as use of a trade mark, but only if a significant number of informed consumers are likely to take that use as a trade mark. On the circumstances of that case, however, the Court held the defendant had not used the plaintiff's trade mark "as a trade mark" and there was no trade mark infringement.

Where to from here?

While the New Zealand position is in contrast to recent developments in Australia, one could speculate that the New Zealand courts may be expected to align themselves with the Australian position in the future, at least in relation to meta tag usage.

This also comes amid growing anticipation of the latest chapter in *Interflora v Marks & Spencer* this year – the colossal battle over the branded keyword INTERFLORA, which extends back to 2008. In November 2014, the Court of Appeal for England and Wales ordered a retrial in the case after setting aside the European Court of Justice's finding that the use of a keyword that is identical to a third party trade mark constitutes use in the course of trade, which is a prerequisite to trade mark infringement. The long-awaited decision is expected to provide definitive guidance on the legitimacy of "sharp" advertising practices by competitors in the online world.

Simply put, advertisers may soon find themselves walking a fine line between hunting clicks and maintaining transparency.

LawNews

LawNews is an official publication of Auckland District Law Society Inc. (ADLS).

Editor:
Lisa Clark

Publisher:
ADLS

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

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

All mail and editorial departments to:
ADLS, Level 4, Chancery Chambers,
2 Chancery Street, Auckland 1010
PO Box 58, Shortland Street DX CP24001,
Auckland 1140, adls.org.nz

LawNews is published weekly (with the exception of a small period over the Christmas holiday break) and is available free of charge to members of ADLS, and available by subscription to non-members for $133 plus GST per year. To subscribe, please email reception@adls.org.nz.

UPDATE FROM ADLS' TECHNOLOGY & LAW COMMITTEE

The ADLS Technology & Law Committee

The ADLS Technology & Law Committee has 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.

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. In this fourth annual special "Technology & Law" edition of *LawNews*, the Committee continues its focus on discussing the impact that new technologies are having on law and legal practice. Recognising that technology has the potential to impact a whole raft of different legal practice areas, Committee members bring together a wide range of backgrounds. Current Committee members are:

Dr David Harvey (Convenor) – Dr David Harvey was appointed as a District Court Judge in 1989, and sat at Manukau for 20 years before transferring to Auckland in 2009. While on the Bench, Judge Harvey was closely involved with information technology initiatives involving the judiciary, including the development of trial management software. Upon standing down from the Bench, he became 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.

Richard Anstice – Richard Anstice is a solicitor at Maude & Miller. He negotiates and advises on a range of commercial transactions, including distribution and IT design and build. Mr Anstice's IT work focusses on the balance between the legal aspects of technology and the practical needs of non-technical people. He can be contacted at richarda@mmiller.co.nz.

Andrew Easterbrook – Andrew Easterbrook works at Rob Harte Lawyer, dealing mainly with technology law, relationship property and estate litigation. He is also a musician and a computer geek. He can be contacted at andrew@hartelaw.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 legal practitioners and policy-makers to develop solutions that focus on access to justice and technology security. He can be contacted at lloyd@gallagherandco.co.nz.

Arran Hunt – Arran Hunt is a technology law specialist at Turner Hopkins. After a decade working as a technical business analyst, for a Fortune50 company in London and several large firms and city councils in Auckland, he was admitted to practise law in 2010. He can be contacted at arran@thlaw.nz.

Melanie Johnson – Melanie 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.

Dr Richard Keam – Dr Richard Keam is a barrister and solicitor currently practising in the area of criminal law, with a focus on crimes involving the use and abuse of technology. Prior to joining the legal profession, he was a professional engineer for 15 years and holds a first class honours degree in electrical and electronic engineering and PhD in electromagnetic engineering from the University of Auckland. He can be contacted at richard@keamlaw.co.nz.

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 since 2000. 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. Mr Lim is responsible for the IT infrastructure and roadmap at the firm and is interested in best of breed legal practice technology that can benefit the firm and its clients. He can be contacted at edwin.lim@hgmlegal.com.

Antonia Modkova – Antonia Modkova is a Trans-Tasman Patent Attorney and lawyer at the intellectual property firm Ellis Terry. She has conjoint degrees Law and Science (Computer Science) and specialises in the drafting and prosecution of software and ICT patents. Outside work, she founded the EduTech startup Osnova, which was accepted into the 2017 Flux Accelerator at The Icehouse. She can be contacted at antonia.modkova@ellisterry.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.

Sophie Thoreau – Sophie Thoreau is a Team Leader and Senior Associate at Baldwins Intellectual Property. She specialises in the strategic use of intellectual property as a business tool, including contentious branding-related intellectual property matters such as copyright, in common law and domain names, in New Zealand, Australasia, the Pacific and internationally. She can be contacted at sophie.thoreau@baldwins.com.

Technology & Law Committee Equal Justice Project (EJP) student representative – The Committee's EJP student representative, Jae Kim, represents 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.

The Committee welcomes any comments, questions or feedback on this special edition, which can be sent to the Committee Secretary at committee.secretary@adls.org.nz.

BOOK

The Future of the Professions

Authors: Richard Susskind and Daniel Susskind

The Future of the Professions explains how "increasingly capable systems" – from telepresence to artificial intelligence – will bring fundamental change in the way that the "practical expertise" of specialists is made available in society.

The book raises important practical and moral questions – in an era when machines can out-perform human beings at most tasks, what are the prospects for employment, who should own and control online expertise, and what tasks should be reserved exclusively for people?

Price: $70.00 plus GST ($80.50 incl. GST)*

Price for ADLS Members: $63.00 plus GST ($72.45 incl. GST)*

(+ Postage and packaging)*

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

Electronic storage of client data and how to not get sued for it

By Andrew Easterbrook, Lawyer at Rob Harte Lawyer

A decade or more ago, it was simple to keep documents secure – keep them where you can see them and lock the door after yourself. It is more difficult today. How do you protect documents when you cannot see them floating away on WiFi signals towards the clouds?

The complexity of an electronic storage system is an order of magnitude (or two) greater than a paper system. Take the simple example of scanning a file using your office copier, instead of taking a paper copy and placing it on the file. Do you know answers to the following: does your scanner email the document or save to a networked drive? If it emails you, what email server does it use? Who has access to the email server? Is it running on a computer which physically belongs to you? If not, who owns it and could they take it away? What software is running on that server? Is it up-to-date? Is the server behind a firewall and if so how is it configured? Has someone changed the default credentials or is access open to anybody who simply asks for it? How long does the server keep copies of emails? Are files transmitted over the Internet or kept within a private network? Are they encrypted in transit? And perhaps most importantly, do you know why you should care about any of that?

We should care. We have obligations relating to the safety and security of client data. Unless we understand the nature and extent of the risks involved in electronic storage, it will be difficult to work out whether we are meeting our obligations. But it is impractical to insist all lawyers must understand exactly how networks and computers function. So this article looks briefly at our obligations and suggests a few easy things to do that will help, even if you do not understand cryptography and subnets and binary solos.

Our obligations about safety and security of electronic data come from a few different areas – legislation, contract and negligence. The most significant legislative requirements are found in the Rules of Conduct and Client care (which deal with confidentiality, security and also require good password management – see rule 11.4), and the *Privacy Act 1993* (principle 5 in particular). There might be some clauses in your retainer that talk about retention, access to and security of electronic data (if not, I suggest you consider inserting some).

Covering all of those areas is beyond the scope of this article. But, while acknowledging the risk of oversimplification, I suggest the following three

Andrew Easterbrook

questions are a good starting point to make sure you are meeting your obligations:

- Have you taken reasonable steps to protect against unauthorised access or disclosure?
- Does your electronic storage comply with your obligation to keep client information confidential?
- Can you ensure that documents stored electronically can be used as admissible evidence?

In this article, I want to elaborate a little on the first question and suggest things that might qualify as "reasonable steps". The hope is that these simple steps will help avoid the risk of complaints or negligence proceedings.

Encrypt data on your devices

Soon (if not already), it will be reasonable to require the encryption of all stored data, wherever stored. Until recently, computers were too slow to make this feasible, at least for data stored on servers. It is close to the point where the effort involved in doing so is no longer such a barrier – if it ever was.

At the very least, if you store any client data on a mobile device or laptop, you must turn on encryption. It is super-easy. On an iPhone, if you use a passcode, then it is probably enabled already. Go to "Settings -> Touch ID & Passcode" to check that "Data protection is enabled" appears at the bottom of the screen. On an Android, go to "Settings -> Security" and turn it on. On a Windows laptop, it can depend on your version of Windows, but to check go to "Settings -> System -> About" and look for the "Device Encryption" section.

Without encryption, if you lose your device, it is trivial for someone to plug the device into a computer and take a copy of its contents, including emails and attachments. You might think that, since you have a password, that is enough. It is not.

If you do not have encryption turned on, you are likely breaching principle 5 of the *Privacy Act* and are probably negligent as well.

Store data in New Zealand, or maybe Australia

Increasingly, firms are starting to use Cloud-based systems. You might find yourself considering an overseas provider, or a provider that stores data or backups overseas. There is nothing inherently wrong with that, but you should be prepared to enforce your rights and your client's rights in the event of a data breach. My view is that, unless you are prepared to file proceedings in America, or Russia, you should not store data there.

The *Privacy Act* is also relevant to overseas storage of data. You should investigate what privacy laws and protections will apply to the proposed overseas storage and consider whether they are adequate. Principle 3 requires you to tell your clients what agency will be holding their information – a good place is in your engagement letter.

Practise good password management

There are lots of myths and bad advice circulating around password management. And, in any event, "good practice" changes regularly. Bearing that in mind, (and you may not want to take my word for this), the following is generally accepted today:

- Do not re-use passwords across different sites, or themes on passwords.
- Use a password manager like "LastPass" or "Dashlane", both of which will automatically generate secure passwords when needed and autocomplete forms, so you do not need to remember your passwords at all.
- If you must commit a password to memory, think of a long but memorable nonsense phrase, take the first letter from each word, capitalise some, and add some numbers or punctuation. For example, the phrase "The Family Court is well resourced to speedily and efficiently deal with all cases, particularly relationship property" could be "TFC-wrtsa3dwac,prp". Obviously, do not use that one, since it is now published and therefore will shortly be added to a database somewhere.
- Where possible, use two-factor authentication.
- Do not write passwords down on paper kept anywhere near your computer.

Evidence

Your clients trust you to ensure anything that might be needed as evidence is admissible.

If you can satisfy the standard used by the *Electronic Transactions Act 2002* (soon to fall under the new *Contract and Commercial Law Act 2017*), that will probably be enough. That test is

Continued on page 5

Continued from page 4

(basically) whether an electronic form of the record "reliably assures the maintenance of the integrity of the information, given the purpose for which, and the circumstances in which, the information is required to be provided or produced". Give it some thought but, as a starting point, I would suggest you ensure that all documents stored electronically have:

- appropriate meta-data – title, description, date, author;
- with scanned documents, a minimum level of quality and a policy that explains what categories should be saved in full colour;
- a flag to show whether an electronic record is a copy made directly from an original document or a copy, and whether the original has been destroyed or retained; and
- some way to prevent alteration or deletion of certain documents (for example, anywhere the "original" flag is present, prevent deletion).

Further reading:

- *NZLS has published guidance on protecting personal information and Cloud computing (see https://goo.gl/prUZKU and https://goo.gl/7MNcCs);*
- *The Privacy Commissioner has some comments on location of data at https://goo.gl/qJTH2Q;*
- *Bruce Schneier is a security expert and has a good blog post on passwords at https://goo.gl/uEPV89.*

LAW AND CYBER SECURITY

What you need to know about ransomware

By James Ting-Edwards, Issues Advisor, InternetNZ

Imagine the moment when, during a demanding day, you are finally back at your computer to finish that one important task. Perhaps you are adding the last affidavit to a document bundle, or giving final approval to a transaction. Your screen awakes with a message: "Oops, your files have been encrypted!" You have been hit with ransomware.

James Ting-Edwards

What is ransomware?

Ransomware is malicious software that blocks a user's access to his or her files and requests payment to re-enable access.

In May of this year, the "WannaCry" ransomware earned global attention, infecting computers around the world. Effects included disruption to hospital and other services in the United Kingdom's National Health Service (NHS).

The WannaCry ransomware exploited a vulnerability in Windows' Server Message Block (SMB) protocol. Microsoft became aware of the vulnerability and issued a patch which fixed it on Tuesday March 14. Prior to the patch, the United States National Security Agency (NSA) had been aware of the vulnerability and had developed a way to exploit it called "EternalBlue". This and other NSA tools were leaked by a group of hackers, the "Shadow Brokers".

What can we learn from this?

With ready access to clever software tools and hard-to-trace online payments, we can expect more creative uses of the Internet for good and ill. On the positive side, there are some relatively simple steps which you and your clients can take to reduce the likelihood and impact of ransomware attacks.

- ***Maintain usable backups*** – Ransomware blocks access to the files on your computer. If you can readily restore those files from elsewhere, a ransomware attack becomes an inconvenience rather than a disaster. We already know we should back up regularly, just as we know we should floss regularly. One way to make this easier is to use Cloud storage (such as Dropbox, OneDrive or Google Drive), or an online backup service (such as BackBlaze or Code42). Cloud data storage is often met with concern. Is it okay to send information to a third-party, perhaps overseas? That concern is proper and should be part of any decision. On the other hand, there are also real benefits to online backups, particularly with respect to ransomware risks. Cloud storage and backup services offer the ability to restore old versions of files. Online providers may be able to detect the mass encryption of your files by ransomware, notice that it fits the profile of an attack, and alert you that this is happening. Finally, Cloud backups can be automated. (As yet, this is not the case for flossing.)
- ***Paying is no guarantee of recovery*** – Paying the amount requested does not always result in restoring access, and identifies the payer as a useful target. In June 2017, another attack based on EternalBlue emerged. The outbreak of "NotPetya" began in Ukraine. Unlike WannaCry, NotPetya asked for payment into the same account for all users. This would make it impossible to unlock a specific user's files, even if the user paid the (relatively low) US$300 amount requested.
- ***Update your software*** – Microsoft fixed the vulnerability behind EternalBlue in March. Systems where all Windows computers were running a fully-patched Windows 10 were not affected by WannaCry in May, or by NotPetya in June. If you run Windows, you should move to Windows 10 as soon as possible. Updating costs nothing but time.
- ***Get credible information from cert.govt.nz*** – CERTNZ is New Zealand's official agency for computer security information and incident reporting. Its website (https://cert.govt.nz) allows you to report incidents and seek help and also shares credible security advice.

Fraud causing headaches for universities

By Melanie Johnson, Legal Counsel, University of Auckland

Implementing technology solutions requires consideration of not only the legal aspects of the implementation, but other factors which may delay or prevent uptake by staff, clients and stakeholders.

Melanie Johnson

Academic fraud is a serious issue for universities, businesses and employers worldwide. Academic fraud includes, but is not limited to, plagiarism, cheating in examinations, fraud in research and falsification of both transcripts and degree certificates. Recent analysis of 5,500 CVs in the UK found that 44% had discrepancies in education claims, with 10% having false grades. Online sites such as "FakeDiplomaNow" make it easy to obtain a fake qualification. The current provision of academic transcripts within Australian and New Zealand universities is still largely dependent on paper-based systems, which are reliant on hard copy documents and therefore open to fraudulent duplication.

Universities New Zealand, representing all eight New Zealand universities, is a signatory to the Groningen Declaration on Digital Student Data Depositories Worldwide (Groningen Declaration). 2017 will see New Zealand universities implementing the Groningen Declaration and rolling out a secure online credential verification service. Through the service, students and graduates will have online access to their records which they can, at their discretion, share with others, including potential employers, professional bodies and other educational institutions.

The service "My e-Quals" is Cloud-based and is built on the concept of "privacy by design", an approach that embeds privacy controls into the technical architecture of the system. The documents are authentic, tamper-proof and legally valid. Documents accessed via the software can only be produced by the participating universities. Students and graduates cannot upload or modify documents in the software. They can only view and share. Employers and others seeking verification of qualifications will be able to check records more quickly and efficiently than is possible through the current paper-based, manual verification process. The underlying systems have been independently tested by security experts and the PDF documents produced through the software contain cryptographic digital signatures that meet the legal requirements set by the European Union for authentic electronic documents, which exceed New Zealand requirements. Access to the service is free for students, whereas paper transcripts incur a charge of $30.

Those New Zealand universities that have implemented the service have met resistance from some organisations, both from within New Zealand and from overseas, and have had to resile from only providing access to academic transcripts through the service. The main problem facing the implementation appears to be a lack of trust in the digital solution. Electronic systems are seen to be vulnerable to hacking and digital documents can be copied and amended seamlessly. This is despite the fact that employers continue to be fooled by fake transcripts and degree certificates. Described below are some of the more recent New Zealand cases in the District Court where job applicants have been found guilty of using fraudulent transcripts and degree certificates to obtain jobs.

In two cases, the defendants obtained senior roles in organisations after presenting false documents. One used a fake degree scroll, which was uncovered after a news report about his appointment included information about his alleged qualifications. The university involved began an investigation and found he did not have the qualifications claimed or any degree. In 2014, another job candidate, when asked for evidence of his academic qualifications as part of the recruiting process, turned to the Internet. He bought a false Bachelor of Laws/Bachelor of Commerce conjoint degree from an Australian university and a Masters of Business Administration degree from a university in Hong Kong. While unsuccessful, he was recommended by the employer for a senior role in a government agency and was subsequently employed on the basis of the qualifications.

It is not only employers, but professional registration bodies, that have been misled. An employee at a childcare centre was convicted and sentenced in the Auckland District Court for forging her childcare qualifications. She had cut, pasted and photocopied documents to make a diploma look genuine and was able to fool the New Zealand Teachers' Council to the extent that it granted her provisional registration.

One professional body which still requires paper-based evidence of completion of the requirements for registration is the NZ Council of Legal Education (NZCLE). Students must provide paper copies of transcripts, despite there being nothing in the regulations or the *Lawyers and Conveyancers Act* which requires this. The Professional Examinations in Law Regulations simply state that a candidate for admission must include with his or her application under this regulation "(a) A certificate or transcript from the university where the student studied for the LLB". Further, section 8 of the *Electronic Transactions Act 2002* (soon to fall under the new *Contract and Commercial Law Act 2017*) specifically states that a document cannot be "denied legal effect solely because it is in electronic form or is in an electronic communication".

The experiences of the universities highlights a problem faced by organisations trying to upgrade their systems and provide more secure and tamperproof storage and retrieval of information. The problem is not just a lack of trust – a whole host of factors come into play when new technology is introduced. In the case of NZCLE, the Application for Admission to the Legal Profession sets out the regulations, but additionally requires that the "documents referred to in paragraph 3 must be original physical (as opposed to electronic) official documents".

Organisations wanting to implement technology solutions need to be aware of what some of the barriers to implementation of technology are. The most famous theory was put forward by the sociologist Everett M Rogers in his fifth edition of the *Diffusion of Innovations*. For Rogers, innovation and technology were synonymous. Technology is composed of two parts: hardware and software. While hardware is "the tool that embodies the technology in the form of a material or physical object", software is "the information base for the tool". Since software (as a technological innovation) has a low level of observability, its rate of adoption is quite slow. Rogers defines diffusion as "the process in which an innovation is communicated thorough certain channels over time among the members of a social system". The four key components of diffusion of innovations are innovation, communication channels, time and social system.

Uncertainty is an important obstacle to the adoption of innovations. An innovation's consequences may create uncertainty. To reduce the uncertainty of adopting the innovation, individuals should be informed about its advantages and disadvantages to make them aware of all its consequences. Diffusion is also a very social process that involves interpersonal communication relationships. For this reason, interpersonal channels are the most powerful to create or change strong attitudes held by an individual.

Organisations face more complex adoption possibilities because an organisation is both the aggregate of its individuals and its own system with

Continued on page 16

TECHNOLOGY AND THE COURTS

The *Electronic Courts and Tribunals Act 2016*

By Dr David Harvey, Director, NZ Centre for ICT Law

The purpose of the *Electronic Courts and Tribunals Act 2016* (Act) is to enable and govern the use of electronic technology in court and tribunal proceedings. It is overarching – all paper-based processes in existing courts and tribunals may be interpreted as allowing electronic processes.

The Act is posited upon the concept of functional equivalence – a theory which gives legal recognition to recording systems and their validation in a format other than paper. The Act in many respects reflects the principles that appear in the *Electronic Transactions Act 2002* (soon to fall under the new *Contract and Commercial Law Act 2017*), which did not apply to the court system.

A central focus of the legislation is upon what is called a "permitted document". The term "permitted document" means a document, including its associated process, in electronic form that is made by, or for use in, a court or tribunal. The purpose of the legislation is to facilitate the use of permitted documents in court and tribunal proceedings and allow existing references in enactments to documents to include permitted documents.

Not all documents are permitted documents and the legislation at section 4(2) lists those that do not qualify. These are:

"(a) a document given on oath or by affirmation;
(b) a statutory declaration;
(c) a will, a codicil, or any other testamentary instrument;
(d) a power of attorney or an enduring power of attorney;
(e) a negotiable instrument;
(f) any notice required to be attached to any thing or left or displayed in any place;
(g) any warrant or other instrument authorising entry into premises or the search or seizure of any person or thing;
(h) any other document specified by the Governor-General by Order in Council made on the recommendation of the Minister;
(i) an item specified in any of paragraphs (a) to (h) that is required to be served by personal service."

The legislation effectively recognises that verification and authenticity of information contained in these classes of documents may only be provided by a tangible paper-based medium.

The Act does not mandate the use of electronic documents, although certain classes of persons yet to be defined in regulations may be required to use them.

The use of permitted documents requires the consent of the person using them, although consent can be inferred from conduct. A person may not be compelled nor directed to use permitted documents. Thus, unless a person consents to the use of permitted documents, it is paper by default.

Dr David Harvey

Where there are requirements for information to be recorded, be in or be given in writing, that information may be in a permitted document, as long as it is readily accessible and useable for subsequent reference. This means that an electronic document must be accessible, in the sense that it is not in an archived or backup format, and can be accessed, presumably in native file format.

The legislation does recognise the dynamic nature of digital information and the reality that multiple copies may be made of a digital document that are identical to the "first" or source copy.

Where there is a requirement that multiple copies of information are to be provided, that requirement is met by providing a single electronic version of a permitted document. A requirement to provide information in a manner that complies with a paper-based form is met by permitted document if information is readily accessible and usable for subsequent reference (see sections 14 and 15 of the Act).

Authentication and signature requirements provide a challenge for those used to verification of a document or its contents by a physical kinetic act, such as affixing a seal or sign manual. How is that accomplished in a digital context?

Signature requirements for permitted documents are addressed in section 16 of the Act. An "electronic signature" or verification must adequately indicate the approval of the information and must be "as reliable as is appropriate given the purpose for which, and the circumstances in which, the signature is required".

Importantly, electronic verification of a document is subject to an exception when one is witnessing a document. According to section 17, witnessing requirements in a permitted document are met by an "electronic signature" if:

- the e-signature complies with the requirements of section 16;
- the e-signature adequately identifies the witness and indicates that the signature or seal has been witnessed;
- the e-signature is "as reliable as is appropriate given the purpose for which, and the circumstances in which, the signature is required".

If a permitted document requires a seal, that requirement may be met by an electronic seal if:

- the seal adequately identifies the party attaching it; and
- the seal "is as reliable as is appropriate given the purpose for which, and the circumstances in which, the seal is required".

The language echoes that dealing with electronic signatures. It is to be noted that the requirements for electronic signatures and seals refer to the issue of reliability. Section 19 of the Act sets out certain presumptions as to reliability (compare this with section 24 of the *Electronic Transactions Act 2002*). An electronic signature is presumed to be reliable if:

"(a) the means of creating the electronic signature is linked to the signatory and to no other person; and
(b) the means of creating the electronic signature was under the control of the signatory and of no other person; and
(c) any alteration to the electronic signature made after the time of signing is detectable; and
(d) where the purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable."

However, any other way of establishing reliability is not excluded and may be used.

The Act also sets out rules for the retention of permitted documents (see sections 20 to 26) and for the dispatch and receipt of permitted documents (sections 29 and 30). These provisions duplicate the provisions of the *Electronic Transactions Act 2002*. The filing requirements (see sections 31 and 32) dispense with the requirement that a document be filed in a particular office of the court and allow for the filing of a permitted document at any place specified in the regulations. In addition, the place for filing may be physical or electronic, and may be centralised or located within the jurisdiction of the court or tribunal.

Some important observations need to be made.
Continued on page 9

Intellectual property rights and the sharing economy

By Sophie Thoreau, Team Leader and Senior Associate, Baldwins Intellectual Property

In recent years, the Oxford Dictionary has added the phrase "sharing economy" to its pages. It defines this term as "an economic system in which assets or services are shared between private individuals, either free or for a fee, typically by means of the Internet".

We may be familiar with this definition at a high level (for example, when we think of new enterprises such as the revolutionary property rental service, AirBnb), but the sharing economy is much more complex than its simple definition.

One potential complication of the sharing economy is its effect on traditional notions of intellectual property ownership, characterised by one entity holding an exclusive monopoly over its brands, patents, copyright and other intellectual property. The discussion below looks at how the sharing economy has the potential to challenge traditional ownership and outlines some practical points for protecting intellectual property in this new economy.

What is the sharing economy?

The term "sharing economy" is often used to capture other terms that have been bandied about in recent times, such as collaborative consumption, "uberization" and "P2P" or "peer economy". All of these terms encompass similar features, such as technology, use of social media, environmental sustainability, monetary benefits and community. Global and local businesses are helping consumers share a range of goods, including bicycles, surfboards, text books, clothing, cars and houses. Businesses are also able to reduce overheads by operating in co-working spaces, people are able to borrow funds from other people through peer-to-peer lending, and individuals or start-ups are able to raise funds through crowdfunding platforms (such as Kickstarter). It is estimated that five key sharing sectors globally – travel, car sharing, finance, staffing and music/video streaming – have the potential to increase revenues from roughly $15 billion in 2014 to approximately $335 billion in 2025 (PWC, "Consumer Intelligence Series: The Sharing Economy").

Through sharing goods and services, it is possible in some cases to cut out the "middle man" employer or company selling goods and services, resulting in positive implications for the cost and convenience of these goods and services for consumers. Of course, as with other 21st century developments, there are some perceived drawbacks of the sharing economy, including privacy and data concerns, problems with insurance arrangements, consumer guarantees for goods and services and also the reliability of business relationships based on trust. In the sharing economy, businesses are required to understand the changing expectations

Sophie Thoreau

of their consumers, constantly evaluate how they market and sell their goods and services, and be open to disruption and working within a different business model.

Traditional intellectual property ownership

The unique innovations, goods and services of a business, and the reputation and goodwill a business builds in these, are protected by intellectual property rights such as trade marks, designs, patents and copyright. Intellectual property rights such as these grant the rights-holder an exclusive right to use and develop its intellectual property to the exclusion of others in the marketplace. At first impression, the above-mentioned intellectual property rights may seem contradictory with the idea of a sharing economy, as rights are founded in the monetisation of ownership and a monopoly rather than sharing. However, as intellectual property makes up around 80% of a global corporation's value, it appears an opportunity awaits for businesses to facilitate the sharing of their intangible assets (see PWC report as above).

Branding and trade marks – remaining in control

Branding, and more specifically registered and unregistered trade marks, are signs (i.e. words, logos, symbols, slogans, designs) that distinguish the source of goods and services of one trader from those of others. Trade marks also enable the building of trust in the quality of products from a specific source. As the shared economy is based on notions of trust, it appears trade marks will continue to have significant value in this new economy, provided companies remain in control of their brands.

Brand control is an important business tool but, as the sharing economy develops, this power is being shifted into the hands of consumers. For example, through social media and sharing platforms, brand owners no longer have total control over the representation of their brands and their distribution channels. Where consumers are the source of goods rather than the brand owner, it becomes more difficult for brand owners to protect their reputation and goodwill in goods and services. Furthermore, consumers can post reviews of goods and services on the Internet and these posts have the potential to reach millions of people worldwide. If these posts are negative, the impact on a business is limitless.

Another facet to protecting your brand is policing of the marketplace and enforcement of your intellectual property rights against infringers. With the rise of the Internet and sharing economy, there is greater potential for others to copy brands they see online, or for consumers to imply a false sense of company affiliation through sharing images of them wearing, eating or using a product when, in fact, the brand owner has not authorised such an endorsement. There is also no clear answer to the question of ownership of user-generated content.

Patents – competitors to collaborators?

Patents are the legal rights that protect invention and innovation – and the immense time, effort and cost that goes into this. As the sharing economy progresses, patents are in a constant state of flux. Technology, platforms and legal frameworks are evolving to offer businesses the opportunity to share innovations, while still retaining the value of their underlying intellectual property.

For example, in mid-2017, Google and eight others (including Samsung, LG and HTC) agreed to share patents covering Android and Google apps. Other players are also allowed to join the agreement, known as "PAX". The aim of the agreement is to defend against patent trolls (where one company obtains the rights to a patent in order to profit by means of licensing or litigation, rather than by producing its own goods or services), and to ensure "innovation and consumer choice continue to be drivers of the Android ecosystem" (Jamie Rosenberg, Android and Google Play). Another earlier example of a similar arrangement was when General Electric shared its patents with innovation platform, "Quirky", and innovators were free to use any of General Electric's patents to develop their own devices. In return, Quirky and General Electric profited from a joint-venture arrangement with the launch of successful products, such as a smart-phone controlled window air conditioner (see PWC report as above).

In both of these situations, the intellectual property owner, through sharing, is able to profit from co-branded product development and increase revenue from its existing intellectual property. Further, by opening up patents to inventors, this has the potential to inspire new ideas, accelerate innovation and provide consumers with access to new products a lot faster than if the intellectual property holder worked independently.

Practical considerations for protecting IP in the sharing economy

Overall, as we can see from simple examples

Continued on page 9

Continued from page 8, "Intellectual property rights and the sharing economy"

related to trade marks and patents, the sharing economy is changing how innovation and intellectual property are approached. Here is some advice for intellectual property owners operating in the sharing economy:

- Companies should take a fresh look at their brand and their products, weaving sharing into the consumer experiences they are creating and considering new marketplaces, business models and consumer values.
- Companies can remain in better control of brands by monitoring distribution of their products, protecting themselves from false endorsements or affiliations and remaining vigilant to trade mark infringement (such as domain squatting or counterfeit products).
- Companies can employ modern marketing tools and engage directly with consumers via social media channels, assisting in the control of brand image and also establishing a community around a brand.
- Leveraging existing and new intellectual property through collaborating with other companies and using technologies that allow for sharing will enable innovators to profit from their intellectual property with greater efficiency and potentially less cost.
- Business relationships need to be backed by watertight licensing and other legal agreements.
- Companies should seek strategic intellectual property advice early in the ideation phase.

***Continued from page 7, "The* Electronic Courts and Tribunals Act 2016"**

Although the Act has commenced, it is not operative. Section 6 requires the Governor-General, by Order in Council made on the recommendation of the Minister, to specify the courts, tribunals or particular jurisdictions of courts and tribunals to which the Act applies. As matters stand, no such Order has been made. Once proper systems are in place to handle electronic filing, the necessary orders will be made.

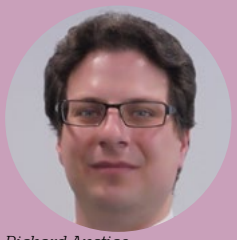
Will the Act significantly change court processes? Except for the changes to place of filing rules, things will largely remain the same. This is because the legislation is imitative of existing processes. Imitative use of technology preserves existing processes and procedures but allows the same objectives to be achieved by electronic means. On the other hand, the innovative use of technology allows for the introduction of disruptive and different procedures and processes enabled by the new technologies which ultimately result in a transformative and improved outcome.

Thus the legislation maintains the model of the paper-based court system and adds a limited form of digital communications in the form of permitted documents – an electronic equivalent of paper.

LAW, TECHNOLOGY AND RISK MANAGEMENT

Emailed payment instructions increase risk of fraud

By Richard Anstice, Solicitor, Maude & Miller



Richard Anstice

Today, all lawyers must rely on a range of information that is often received by email. This includes relying on emailed information to initiate payments out of trust accounts. Email information is often reliable, as long as the sender's and receiver's email accounts are reliable and have not been hacked.

However, there has been and will be continuous growth of hacking and fraud techniques that intercept legitimate emails and replace them with fraudulent emails. If payment details are not checked, this creates a risk that funds are paid out to fraudsters. Managing this requires all lawyers to continuously review the reliability of the information they receive by email.

Across all business sectors, New Zealand banks and insurers are increasingly aware that email interception and provision of fraudulent payment details by email are key risks.

Consider this scenario. Your firm receives bank account information for a payee by email. Before paying money out of your trust account, how often have you used the telephone or fax machine to verify a payee's bank account number? Always? Rarely? Never?

In the United Kingdom, *The Telegraph* has reported at least two examples of payments made to the wrong bank account due to fraudulent emails. In one case, the solicitor for a purchaser had his email account hacked. The lawyer attempted to email payment instructions to the purchaser and pay funds necessary for the purchase. The fraudster intercepted the lawyer's payment instructions and substituted a fraudulent email with his own details. The email looked genuine, and resulted in the client paying more than £200,000 to the fraudster's account. The funds were not recovered.

In another conveyancing case, the vendor's solicitor had emailed the vendor asking for bank account details to pay out the proceeds of sale. The vendor's email account was hacked and the email intercepted. A fraudulent email was substituted, and the solicitor paid out the settlement funds to a fraudster's account. There was only a partial recovery of the funds.

Recommended actions to better protect trust accounts against this high-tech fraud include:

- ***Collect and give out bank account details face-to-face during initial meetings.*** During initial client meetings, standard practice is to verify clients. Even if payments will not be made until the end of the transaction, the initial meeting is often the most secure forum to collect payment information.
- ***Telephone the payee and ask him or her to read to you the correct bank account details.*** Find the phone number from an independent source (not the email footer to the same email). If possible, staff members who recognise the client's voice should make the call.
- ***Contact the payee using a reliable fax number.*** Particularly when dealing with other solicitors, a fax number can be found from a mailed letterhead or similar reliable documentation. It is better to find lawyers' contact information on the Law Society's register, rather than a firm's website (some firms' websites may be more vulnerable to hacking).
- ***If possible, ask payees to bring payment information in person.***

Above all, encourage staff to check, verify and double-check. In case of doubt, all staff should know to delay payments.

Protecting lawyers' trust accounts is more than just a matter of avoiding loss of money. It is about trust. To maintain the reputation of the legal profession as transaction experts, we must always show we are the best at managing online security. This requires that lawyers always use the best possible processes to protect from online security threats.

Android v Apple – A tech lawyer's perspective

By Arran Hunt, Technology Law Specialist, Turner Hopkins

As a disclaimer, I use Android products. My last four phones have run Android, my watch runs Android, my TV runs Android, even my car stereo runs Android. It has been several years since I have owned an Apple product.

However, with smartphones being such an important part of our everyday life, I feel that it is necessary to look at which is the better option for lawyers. This is generic advice. You may have a reason not included below for why you must run one or the other. However, hopefully the list below provides some help.

We will look at several categories here.

Size
There has been an ongoing move to larger phones. Size has typically referred to the diagonal screen size, with bezels becoming noticeably reduced. With phones like the Samsung S8, the screen now takes up 83% of that side of the body. By comparison, the iPhone 7 plus is 67.7%.

Apple have a range of sizes from the iPhone SE at 4", up to the iPhone 7plus at 5.5". The upcoming iPhone 8plus is rumoured to be 5.8" and should have a screen to body ratio to match the S8.

Android has dozens of makers with hundreds of current phones. The Unihertz Jelly has just been released with a 2.45" screen. The largest was the 2015 Huawei P8 Max at 6.8", with several current phones not far behind in size.

With a wider variety of sizes, Android wins.

Price
Apples are notoriously expensive. While many will defend the pricing as being justified, you do not become the world's largest company by just breaking even.

Android phones come in a wide variety of prices, from as low as $20-$30. They can go up to Apple level prices, but have a price point for just about every user.

With a range of prices, Android has the advantage here.

Features
With a small number of phones, there is little option as to which features you will or will not pay extra for when buying from Apple. However, its phones are all reasonably feature rich. Apple will, however, lock some of those features down, permitting you to use them only how Apple dictates. A prime example is the NFC (near field communication) where it is only currently available to Apple Pay. In an Android phone, NFC can be used for a variety of purposes.

With a wide variety of phones, Android users can look as to what features they want to pay for. The high-end models will have features comparable to the Apple phones. Mid-range phones allow users to drop those features that they do not see as important. There are also phones with specific features, such as the Motorola Moto Z with its clip-on features (such as a Hasselblad camera lens), or the upcoming Red phone with holographic screen.

Arran Hunt

For a wider variety of features, and the choice of which phone to buy to gain which features, Android wins this category.

Applications
Both platforms have a market – App Store for Apply and Google Play for Android. Both were launched in 2008. By 2016, Google Play had a larger number of apps available, and a larger number of application downloads – 64 billion compared to the App Stores 25 billion.

However, the larger number of apps on Google Play is largely due to an easier publishing regime. Google Play has become notorious for useless apps that have no real purpose. Even worse, there have been several occurrences of malware slipping in to apps available on Google Play and ending up on user's phones. While the same issues have occurred with the App Store, they occur much less frequently, as each application must go through a more rigorous screening process.

Apple users, having already purchased what was most likely a more expensive device, are also more willing to spend money on apps, leading to the App Store having a turnover that is 60% higher than Google Play. This leads to more specialist developers developing applications aimed at professional roles. As a result, you are more likely to see practice management software having apps on the App Store than on Google Play.

With better security, higher quality average app, and better support from legal software developers, this is Apple's win.

Modifications
Apple controls its phones. What the user can and cannot do is set by Apple.

Android is not as locked down. Simple items, such as changing the onscreen keyboard, can be done in seconds. While some protection from more intensive modification exists, some manufacturers (such as Sony) provide instructions on how to remove them. The user can then replace the software completely with one of a range of modified operating systems available online.

For lawyers, Android's approach is problematic. While small modifications to the user interface are nice, we need some level of confidence that other changes have not been made. The ability to "sideload" apps (installing apps that did not come through Google Play's review process) creates an inherent security risk the moment our phone is not in our control.

For a lawyer, this is a win for Apple.

Security
Both platforms allow for security software to be installed, so that is not an issue, and every lawyer should have such software on their phone. However, Android's approach of allowing open use of the software by multiple manufacturers, on hundreds of different phone models, has created a major security issue.

Whenever a security flaw is found, Apple and Google will be hard at work fixing it. However, when a solution is found, their method of implementation will differ greatly. Apple will roll it out to the phones it still supports (typically the previous two generations), so that those users are protected. As this is a small limited number, it is easy for Apple to modify the fix to work for each phone type.

Google must go through a different approach. As there are too many different phone models running its software, Google will release an update to each of the phone manufacturers. It is then up to that manufacturer to modify the update for the models they sell, before releasing that update to their users. For most manufacturers, this may only happen for their latest model, if at all. For others, such as Samsung, this could take some time. I currently use a Samsung Note 5, which received an update to Android 6 in March 2017, almost two years after Google had released it, and nine months after Google had released Android 7.

For a lawyer, with a need to be patched and secure from any new issues, this is a win for Apple.

Recommendation
Apple.

I love Android and Google. However, for a lawyer, security of emails and client information must come above all else. Apple won every category that counts.

My next phone will be an Apple, perhaps the iPhone 8plus that releases later this year. Until then, I will have to see if I can borrow an Apple from someone.

AI AND THE LAW, LEGAL PRACTICE

Artificial Intelligence in practice

By Dr David Harvey, Director, NZ Centre for ICT Law

A considerable amount has been written about Artificial Intelligence (AI) and the way that it is going to change work habits and practices.

To put AI into context, it is no more and no less than an aspect of the digital paradigm which itself is disrupting and transforming society. AI is something of a "dog-whistle" issue, giving rise to images of robots and disembodied voices telling humans what to do. This is an aspect of what the science fiction author Isaac Asimov referred to as "The Frankenstein Complex" – the atavistic fear of the created being.

Asimov did very well out of the Frankenstein complex. His series of "robot stories" were premised on some of the paradoxes that arose from his "Three Laws of Robotics", which were designed to keep humans safe from the machines. All his robots were programmed with the Three Laws, which read thus:

- a robot may not injure a human being or, through inaction, allow a human being to come to harm;
- a robot must obey the orders given it by human beings, except where such orders would conflict with the First Law; and
- a robot must protect its own existence, as long as such protection does not conflict with the First or Second Laws.

Asimov's paradoxes in his stories were in fact not science fiction, but exercises in statutory interpretation. Others have also done rather well from the Frankenstein complex (one only has to look at the success of the "Terminator" franchise). But rather than speculate about where AI is going, perhaps we should look at the AI that is with us and how that is going to impact on legal practice. Rather than worry about how we are going to regulate, inhibit or otherwise emasculate AI, we should be asking how lawyers can use AI systems to improve their practice and their services to their clients.

The deployment of AI into law has been with us for some time. That it should extend further is inevitable. But this does not mean decisions by Terminator J. Rather, use of AI systems will enable the smarter use of lawyer's time and expertise. It will free lawyers up from repetitive tasks and enable far more targeted advice based on more accurate data analytics. AI is already being used in e-discovery using a number of different systems, of which predictive analysis is becoming well-known.

I want to briefly describe one subset of AI – legal expert systems – and place it within the context of the law office.

Dr David Harvey

Legal expert systems

An expert system is a system that is "capable of functioning at the standard of human experts in a given field" (John Zeleznikow and Dan Hunter "Building Intelligent Legal Information Systems in the Law", H.W.K. Kasperson et al. eds., Kluwer Computer Law Series 13 1994 (see pages 4 and 69)).

Expert systems enable many people to benefit from the expertise and judgement of experts anytime, anywhere, cost-effectively. They create leverage at Internet scale. However, one must use the term with some care, for it may encompass a number of different ways in which computer algorithms may be deployed.

Expert systems fall into four major areas:

- ***Analysis and advice*** – Systems basically set up to provide answers to questions based on an "IF THEN" model. A fact-specific analysis is required and it must be clear how the system reached its conclusion.
- ***Intake and assessment*** – These guide users through a system that collects data, evaluates facts and issues, and recommends actions to the user. Examples may be an incident reporting system, a compliance review system, a claim evaluation system or a due diligence guide.
- ***Intelligent workflow*** – These can be long running sessions. Rules are applied and messages are sent to multiple parties who contribute to the system and, when all the facts are gathered, reasoning is completed and the workflow is completed. Examples may be a process management system, a leave request manager or a compliance authorisation system.
- ***Document automation*** – These leverage the software to create complex documents of many types, including complex legal documents.

Generally, fact values may be obtained from the user or sourced externally from databases, files, web service or other applications. The expert system software applies fact values to reasoning and sets conclusion values. This process continues and, when all the required values are generated and sent, databases are updated and the session is complete.

Applications for legal expert systems

Information retrieval systems and expert systems comprise two types of AI applications used in law. Legal expert systems' designs are categorised as either case-based or rule-based systems. Often, researchers build systems on a combination of the rule-based and case-based approaches. Rule-based systems are the most prevalent legal AI expert systems. These systems store legal knowledge as rules. The rule-based systems reason directly with these legal rules through formal logical deductive and inductive methods. Case-based systems operate by comparing the intersections of facts in a database of past cases, called exemplars, with the facts in the present situation. The case-based system attempts to draw analogies between the exemplars and the present case in order to retrieve the most on point cases.

Lawyers were originally identified as primary target users of legal expert systems. Potential motivations for this work included:

- speedier delivery of legal advice;
- reduced time spent in repetitive, labour intensive legal tasks;
- development of knowledge management techniques that were not dependent on staff;
- reduced overhead and labour costs and higher profitability for law firms; and
- reduced fees for clients.

Later, work on legal expert systems has identified potential benefits to non-lawyers as a means to increase access to legal knowledge. Legal expert systems can also support administrative processes, facilitating decision making processes, automating rule-based analyses and exchanging information directly with citizen-users. The benefits for clients are improved outcomes, reduced risks and reduced costs. For the experts in the domain new revenue streams are generated, strengthened and improved client relationships and replacement of billable hours with applications.

Commoditising advice

As noted, legal expert systems allow the repetitive aspect of legal work – gathering information and applying fixed criteria to ascertain rule application – to be automated. But the automation process is not "bespoke". It has standardised elements to it and is therefore reusable. Because it is reusable, it can be considered a commodity.

Continued on page 16

VOIP fraud and the *Telecommunications Act 2001*

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

Over the past year, New Zealand has seen a considerable rise in fraudulent telephone calls that use Voice Over IP (VOIP) technology.

These calls are generally originated offshore by a party which obtains a New Zealand number that it then routes into its VOIP PBX (a "VOIP PBX" is essentially a computer running a VOIP PBX software, such as "freePBX", that allows for the translation of the VOIP number to the standard telephone network).

This technology has a range of advantages in legitimate circles – e.g. for cost-cutting, as well as flexibility for communication while abroad. However, those misusing the technology have taken these legitimate services and adapted them to engage in actions that have resulted in ransomware attacks, as well as simple fraud attacks for pecuniary advantage.

A standard VOIP attach usually proceeds as follows:

- Party A (the mischief-maker) obtains a New Zealand number and uses it in its VOIP PBX to initiate a call with a New Zealand caller ID to Party B (the unsuspecting party);
- Party A claims to be, for example, from Inland Revenue (a matter unsuspected because of the 04 or 03 area code appearing on caller ID), and advises that Party B is facing prosecution for an alleged breach of tax legislation;
- Party A then advises that such action can be prevented by Party B paying a certain amount to Party A by credit card or wire transfer. In some cases, Party A will request information instead (if the fraud is for another purpose), but most of the time the aim is to obtain quick cash from the unsuspecting. Due to the low nature of the sums sought, and the consumers' lack of knowledge (for example regarding IRD procedures), many consumers simply pay the fee.

Scams of this kind have occurred nationwide and range from the example above to claims of prosecution that can be resolved by paying a fee/ fine, to (my favourite) calls purporting to be from Microsoft technical help desk showing that your computer is reporting infection, whereby they ask you to install a virus/malware cleaner that is in fact ransomware. The plausibility of this scam is assisted by the fact that Microsoft, while marketing Windows 10, stated that error reports would be sent to Microsoft for evaluation, thus opening the door to potential VOIP fraud. (Note: the reason that the Microsoft scam is my favourite is because it shows the scammers' lack of prior investigation when they call my offices, where we advertise our worldwide expertise.)

Lloyd Gallagher

What these examples show is that the way companies are advertising their services is opening the door to this new fraud. And users have reported that, when making complaints about the number abuse, they have to go through several steps to report the issue to their telecommunications companies that are often cumbersome.

So, what can be done?

The abuses mentioned above fall under the misuse of network provisions in section 112 of the *Telecommunications Act 2001* (the Act). Section 112(2)(b) makes it an offence to use a "telecommunications device" knowingly to give factitious information, orders, instructions or messages. "Telecommunications device" is not directly defined in section 5, but has been interpreted by the courts as including a "telephone device", which does have a definition under that section. Unfortunately, VOIP technology falls outside this scope, as it does not connect to the network in the traditional way, as per the courts' reading of "telephone device" (see *Powel v Police* [2000] 3 NZLR 98). These questions have prompted debate internationally as to where VOIP sits and whether law reform is needed to categorise it as a new class (see discussion papers by the International Telecommunications Union (ITU) mentioned at the end of this article).

The use of VOIP to obtain pecuniary advantage appears to be a clear breach of section 112(2)(b), suggesting that the inclusion of VOIP technology under the section 5 definition would be appropriate.

"Telecommunication" is defined in the Oxford English Dictionary as follows: "n. communication over a distance by cable, telegraph, telephone, or broadcasting", while the entry for "Telecommunications" reads "[treated as sing.]: the branch of technology concerned with this".

The ITU defines "VOIP" as technology based on different signalling and communication protocols. It works by sampling the sound by a computer at very high rates (at least 8,000 times per second or more) and recording or storing these samples. The computer then compresses the sound, so it requires less space, using a compressor/ de-compressor algorithm. Once recorded and compressed, the sound is collected into larger data packets ("packetisation") and sent over the IP network. VOIP is then transmitted over the network from PC to PC (such as Skype), IP phone to IP phone (such as Cisco SPA962), or IP phone to gateway (this is a PBX or adapter which allows for the IP call to be connected to the PSTN (standard phone network)).

Standard telephone devices are designed to carry 64KB traffic signals bidirectionally in a raw uncompressed data stream over the copper lines using techniques of modulation and codecs. They use a standard telephone apparatus that modulates the audio. The call is then carried over the PSTN using a 64 kbit/s channel. The name given to this channel is Digital Signal 0 (DS0). The DS0 circuit is the basic granularity of circuit switching in a telephone exchange. The broad wording of telecommunications device in this section does not appear limited and would arguably include the use of a computer to send an email or other message over the Internet. Accordingly, as both VOIP and PSTN networks use standard transmission techniques for voice communications that, today, include a wide range of codecs to send messages, albeit in message packets, VOIP would fall within the definition of telecommunications device and prosecution should be available for VOIP fraud.

However, enforcement may be difficult, as many of these frauds originate offshore and also due to the requirements under the number portability scheme that parties share numbers across all providers. While changes in policy to restrict VOIP numbers may provide some assistance, this will not resolve the issue, as some New Zealand customers are obtaining New Zealand numbers to hold in their names and resell to third parties to use them on VOIP networks.

I would suggest that better protection is needed at telecommunications company level, including improved complaints and reporting procedures, and more robust validation procedures for persons obtaining numbers. However, I would also caution that a balance is needed in terms of validation procedures, as a too-restrictive environment will unduly hamper legitimate users of this new technology.

Further reading:

- Powel v Police *[2000] 3 NZLR 98;*
- Joy v Police *[1994] NZFLR 865;*
- *https://www.itu.int and https://www.itu.int/osg/spu/ni/voice/papers/FoV-VoIP-Biggs-Draft.pdf;*
- *http://www.stuff.co.nz/business/industries/81187263/is-nz-too-free-with-its-phone-numbers.*

CRIMINAL LAW AND TECHNOLOGY

Some implications of augmented/virtual reality on criminal law

By Arran Hunt, Technology Law Specialist, Turner Hopkins

I am not a barrister, and this is not intended to be a training document to others in my field. This article proposes some small legal issues that virtual reality (VR) and augmented reality (AR) may create in relation to criminal law.

In time, I hope to research these areas in more depth. My hope is that, with some forethought, the industry can be prepared with applicable legislation in place. At worse, it will see some interesting arguments in court.

Evidence

There is a concept in several industries called the "uncanny valley". For years, we have watched movies with effects that now seem childish, yet our minds made them real. As those effects improve, our minds rebel. It stops making the images seem real. Instead we feel nothing for the characters, they seem off, and we can even feel revulsion for them. This is the "uncanny valley" – that final hurdle to making what we see seem real. With recent developments in technology, the uncanny valley will soon be bridged. What you see will seem real.

Augmented reality works through superimposing images and audio onto the real world. Someone wearing an AR headset will see, as normal, what is in front of them. The headset will project images on top of that, thus "augmenting" reality. Most of what the viewer sees is real and not a projection. The rest is computer-generated, transferred to the headset from a PC. Many futurists believe that augmented reality will become as common as a smartphone (https://goo.gl/MNvcXG shows one possible future).

As AR improves, and the uncanny valley is passed, what is being superimposed will become indistinguishable from what it overlays. Our only way to perceive that it may not be real is that it does not fit into how we perceive the world. For example, a four-foot-tall talking duck sitting on my desk would be an augmentation of reality, no matter how real it looks. However, what if it was not a talking duck but rather someone admitting to a crime? Or perhaps someone committing a crime? From the witness' perspective, they saw the crime. They may have heard it. They would not be lying by saying they saw something happen and heard a confession, but was it reality? If they are wearing an AR headset, fed by a PC that could have been compromised, how reliable is their evidence?

Terror

One of the main reasons for VR/AR is to create immersion. While a television or a film can be engrossing, there is no control by the viewer – you feel for the protagonist, but you are not the protagonist. Video games have brought the gamer more in to the equation, giving the gamer active control of the protagonist.

Arran Hunt

> As AR improves, what is being superimposed will become indistinguishable from what it overlays. Our only way to perceive that it may not be real is that it does not fit into how we perceive the world.

There has also been a long conversation about whether violent films and video games have an impact on behaviour. As a way to prevent the worst from being experienced, the *Films, Videos, and Publications Classification Act 1993* provides a framework through which films and games are classified if they are deemed objectionable. Section 3 of that Act defines what is objectionable. The aspect of the definition that deals with violence is "acts of torture or the infliction of extreme violence or extreme cruelty". All other mentions of violence are related to some other factor, such as sex, children or being directed at a particular class or group.

Section 3B allows for a further class which "describes, depicts, expresses, or otherwise deals with harm to a person's body whether it involves infliction of pain or not ...". Section 3B allows for an age restriction to be imposed. The Act therefore allows for restrictions to be implemented when violence is depicted. To date, nine video games have been banned in New Zealand. All involved video games in which the player was required to act extremely cruelly towards the in-game characters. None relate to the viewer experiencing that horror. They also require some level of cruelty and violence to be portrayed.

Such violence and cruelty is not required to create a horrifying experience. Imagine an experience where an AR headset would put random shadows and sounds in to your everyday life, building up the belief of a sinister presence in the viewer's house. It could be subtle enough that the viewer does not automatically realise that it is the software. It could even be installed in a way that a viewer does not even know it is running. Some may find such a situation exhilarating. For others, it could remove the security they find in their home, and may lead to more serious mental health issues. Those "voices in your head" could be more suggestive and come from an outside source without the viewer realising.

The *Films, Videos, and Publications Classification Act* would not necessarily catch some of those games, as there is no inherent cruelty or violence being depicted. Instead, they deal in horror and fright. Killing through fright is a crime under sections 160 and 163 of the *Crimes Act 1961*, however, the developer will most likely be too far removed to be culpable, or would likely be in another jurisdiction. If the harm did not lead to death, then such sections are not applicable, with nothing explicit to take their place. If such software was installed without the viewers' knowledge, then there could be action available under section 249 (if the harm can be shown to be a loss) or section 250 of the *Crimes Act*. Perhaps, instead, the approach should not be on what can be provided, but, rather, what can be used.

In a world with the immersion that VR/AR provides, should there be a limit of what someone can agree to endure? The case of *R v Brown* ([1994] 1 AC 212; *R v Brown* [UKHL] 19) is one that many of us will remember. It looked at consent in relation to assault – what could someone agree to. Its focus was on actual bodily harm. However, as mental harm is not as defined a crime as assault, neither court gave any real consideration as to whether someone could consent to what could be a mental harm. If there was ever an instance of the death of a child (or a vulnerable adult) due to a VR/AR game, such a limit may need to be defined by the court if it has not been covered in legislation.

AR/VR use is growing. With nearly every smartphone being able to provide a VR experience (just by putting it in a $20 headset), its use will become commonplace. These are just some of the implications that we may expect to see.

Featured CPD

Family Business Succession: Asking the Right Questions

Globally around 80% of businesses are family owned and run. In New Zealand and globally, only 25 to 30% of businesses are successfully transferred to the second generation. Creating a succession plan that works best for all family members involved requires a multi-disciplinary approach. There isn't a master plan that suites everyone, but rather each client will require their own bespoke approach. This Forum takes a holistic approach on planning for family business succession by highlighting the issues you need to address, questions you should be asking and the different advisers you should be engaging with.

Learning Outcomes:

- Gain an increased understanding of 'Better practice' for good governance and its role in succession.
- Learn more about the different aspects of succession and receive practical advice on what you need to do to in order to create an effective exit plan.
- Gain insights on strategies and suggestions for dealing with the challenges of advising a family business.
- Receive an introduction to The System's Theory Model of Family Business.

Who should attend?

All lawyers representing owners of small businesses. Accountants, trust lawyers and those involved in estate planning may find this useful.

Forum **Livestream**
CPD 2 hrs

Tue, 5 Sep
4pm – 6.15pm

Presenters
Dr Deborah Shepherd, Senior Lecturer, University of Auckland

Darren White, Head of Family Business Services, EY

Atul Mehta, Director, Moore Stephens Markhams

Chair
Catherine Atchison, Partner, Martelli McKegg

Rural Law Series: Overseas Investment in the Rural Context

Overseas investment is often a contentious issue and never more so than in the rural sector. This webinar will consider recent developments in overseas investment, look at relevant case law and the particular issues that arise in the rural context and provide advice on how best to represent clients when dealing with the Overseas Investment Office.

Learning Outcomes:

- Learn more about recent changes to the OIO's operations, including revised application processes and templates, increased monitoring and enforcement of consent conditions, and good character developments.
- Gain insights into judicial consideration of the Overseas Investment Act, including counterfactual requirements, application of the associate provisions and the treatment of certain interests in land.
- Increase awareness of specific rural issues as they relate to overseas investment.

Who should attend?

Rural law practitioners and other practitioners who might advise on OIO matters generally.

Webinar
CPD 1 hr

Wed, 13 Sep
12pm – 1pm

Presenters
Phil Taylor, Partner, Tompkins Wake

Campbell Stewart, Senior Associate, Tompkins Wake

Non-Party Disclosure: Potentially a Powerful Tool

Non-party disclosure can be a powerful tool in a Criminal lawyer's armoury, but it is used less often than it could, or should, be. This seminar will explore the ins and outs of the application, including the legal basis, timing, procedure, hearing, outcome, utility and key case law. With non-party, prosecution and defence perspectives and judicial insights, this session is a must-attend for all Criminal practitioners including youth advocates.

Learning Outcomes:

- Receive guidance on when and how non-party disclosure can be pursued.
- Gain a better understanding of the need for and definition of 'relevance' in relation to an application, and implications for the Court/progression of a case.
- Gain insights into the use of non-party disclosure by the Police and the Crown's position on defence applications.
- Receive practical guidance on how defence can use the information once disclosure is obtained/ implications for case preparation.

Who should attend?

All those practising in Criminal law including youth advocates.

Seminar **Livestream**
CPD 2 hrs

Thu, 31 Aug
4pm – 6.15pm

Presenters
Chris Holdaway, Senior Solicitor, Ministry of Social Development

Gareth Kayes, Director, Kayes Fletcher Walker Limited

Belinda Sellars, Barrister, 22 Lorne Chambers

Chair
His Honour Judge Hinton

Agreement for the Sale and Purchase of a Business

A revision of the ADLS/REINZ Agreement for the Sale and Purchase of a Business is soon to be released and it is important that transactional lawyers familiarise themselves with it.

This webinar, presented by the drafters of the revision, provides an excellent opportunity to learn more about principal changes, the reasons behind the changes and what they will mean for both vendors and purchasers. There will also be a discussion about the GST implications for business sales, with particular reference to zero rating rules.

Learning Outcomes:

- Learn more about what is new in the latest Agreement including new GST wording, provisions for covenantors and guarantors in cases where parties are incorporated entities and personal covenants are required, as well as improving lease assignment obligations new warranties, restraint of trade and dispute resolution wording and allowing purchasers the opportunity of pre-settlement inspection.
- Discuss the new due diligence clause and how an effective "DD" investigation should proceed.
- Gain insights into the GST requirements for business transactions, including the requirements for zero rating and CZR and how they operate in the context of a business sale.

Who should attend?

All commercial lawyers involved in the sale and purchase of businesses and general practitioners who do commercial law work from time to time.

Webinar
CPD 1.25 hrs

Wed, 30 Aug
12pm – 1.15pm

Presenters
Chris Bradley, Director, Carson Fox Legal

Allan Bullot, National Indirect Tax Lead Partner, Deloitte

CPD in Brief

ADLS/SCA(NZ) Unit Titles/Bodies Corporate Half-Day

ADLS and SCA(NZ) will be holding their inaugural half-day conference on issues relating to unit titles and bodies corporate. With input from lawyers and property managers this event will cover a range of topics relevant to all those who have dealings in this area of law.

Early bird rates available before 8 September 2017

Conference
CPD 4 hrs
Thu, 21 Sep
12.30pm – 5pm

Leading Your Career – Exclusively for Women Lawyers (Auckland)

Take charge of your career and realise your underlying potential. This practical, interactive one-day workshop, led by one of New Zealand's top female lawyers and one of New Zealand's top leadership experts, will arm you with resources, self-confidence and focus to apply immediately to your role and to enhance your future career.

This workshop is normally only available as an in-house programme for law firms.

Places are limited. Previous workshop was over subscribed. Register now to avoid missing out.

*CPD hours: 7 hours onsite (excluding breaks) plus a preparatory 1 hour online assessment

Presenters: Miriam Dean QC: **Liz Riversdale**, Director, Catapult Leadership Training

Workshop
CPD 8 hrs*
Wed, 13 Sep
9am – 5pm

Negligent Misstatement – Where Are We and Where To From Here?

Negligent misstatement effectively subsumes all types of negligence in New Zealand, and in many cases the defendants are lawyers! Starting with a contextual background, this seminar will focus on recent developments and the road ahead, as well as looking at key concepts and case law, which may assist lawyers to protect themselves and their clients.

Presenters: Andrew Barker QC, Barrister, Shortland Chambers; **Marcus Roberts**, Senior Lecturer, University of Auckland

Chair: The Honourable Justice Davison

Seminar Livestream
CPD 2 hrs
Thu, 14 Sep
4pm – 6.15pm

Commercial Law Series: Directors' Risks: Managing Personal Exposure

Actions can be brought against Directors personally by one or more of the following persons: a shareholder; the Company; a liquidator; a regulator (for example the IRD); and a holder of a personal guarantee.

This webinar will outline those actions, the consequences, and the practical and legal steps a Director can take to reduce the likelihood of a claim being brought, to improve the chances of successfully defending it and to mitigate its impact on their personal assets if the action is successful.

Presenters: Brent Norling, Director, Norling Law; **Christopher Lee**, Partner, Hesketh Henry; **Stephanie Corban**, Senior Associate, Hesketh Henry

Webinar
CPD 1.25 hrs
Wed, 20 Sep
12pm – 1.15pm

Retirement Villages: Advising on the Wisdom of the Transaction

Retirement villages, one of the fastest growing industries in New Zealand, may also be one of the most problematic when advising clients making the move. This seminar will consider some of the areas where lawyers need to be especially vigilant when giving advice to clients and will provide insights into how best to engage with clients in order to protect their interests.

Presenters: Megan Bawden, Director, WRMK Lawyer; **Glen Low**, Partner, Franklin Law

Chair: Troy Churton, National Manager (Retirement Villages), Commission for Financial Capability.

Seminar Livestream
CPD 2 hrs
Tue, 26 Sep
4pm – 6.15pm

CPD Pricing

Delivery Method	Member Pricing	Non-Member Pricing
Webinar (1 hr)	$75 + GST (= $86.25 incl. GST)	$105 + GST (= $120.75 incl. GST)
Seminar (in person)	$125 + GST (= $143.75 incl. GST)	$180 + GST (= $207.00 incl. GST)
Seminar (livestream)	$125 + GST (= $143.75 incl. GST)	$180 + GST (= $207.00 incl. GST)
On Demand (1-hour recording)	$85 + GST (= $97.75 incl. GST)	$120 + GST (= $138.00 incl. GST)
On Demand (2-hour recording)	$140 + GST (= $161.00 incl. GST)	$200 + GST (= $230.00 incl GST)

For group bookings for webinars, seminars & On Demand, see the ADLS website at: adls.org.nz/cpd-pricing.

ADLS Connecting New Zealand Lawyers | airpoints™

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

Continued from page 6, "Academic fraud is a serious issue for universities "

a set of procedures and norms. Organisations can feel pressured by a tension for change. If the organisation's situation is untenable, it will be motivated to adopt an innovation to change its fortunes. This tension often plays out among its individual members. Innovations that match the organisation's pre-existing system, require fewer coincidental changes, and are easy to assess, are more likely to be adopted. The wider environment of the organisation, often an industry, community or economy, exerts pressures on the organisation too. Where an innovation is diffusing through the organisation's environment for any reason, the organisation is more likely to adopt it. Innovations that are intentionally spread, including by political mandate or directive, are also likely to diffuse quickly.

Rogers notes that people acquire knowledge about innovations that are in accordance with their interests, needs and existing attitudes, and seldom expose themselves to information if they do not perceive the need. The need to adopt must be consistent with their beliefs. "[A]ll innovations carry some degree of uncertainty for an individual, who is typically unsure of the new idea's functioning and thus seeks social reinforcement from others of his or her attitude toward the innovation."

If the existing system works well for the organisation, then change may take longer or may not occur at all until the community of practice accepts the new technology. Acceptance may just require time to seep through the complex and often unwieldy decision making processes of large and rule-bound organisations such as universities and professional bodies. There also needs to be acceptance within the wider community of practice that electronic, Cloud-based solutions may be safer and more reliable alternatives to paper-based systems.

ADLS COUNCIL

Contact details for ADLS Council

Here are the contact details for your ADLS Council. They welcome your queries and suggestions.

Joanna Pidgeon (President)
Ph. (09) 337 0826 E. joanna@pidgeonlaw.co.nz

Marie Dyhrberg QC (Vice President)
Ph. (09) 360 4550 E. maried@mariedyhrberg.co.nz

Tony Bouchier
Ph. (09) 623 1772 E. bouch@xtra.co.nz

Vikki Brannagan
E. vikki.atack@gmail.com

Craig Fisher
Ph. (09) 367 1654 E. craig.fisher@rsmnz.co.nz

Tony Herring
Ph. (03) 377 2900 E. tony@mmlaw.co.nz

Stephanie Nicolson
Ph. (09) 309 2500 E. sjn@lojo.co.nz

Mary Anne Shanahan
Ph. (09) 827 6106 or (09) 827 2783 E. mary@shanahanslaw.co.nz

Bernard Smith
Ph. (09) 355 0088 E. bernard.smith@dawsonharford.com

Continued from page 11, "Artificial Intelligence in practice"

This concept of the commoditisation of legal work is discussed by Richard Susskind in *Tomorrow's Lawyers, 2nd Edition* (Oxford, 2017) (see chapter 3, page 25 et seq). The standardisation element means that repetitive tasks can be systemised, because in many respects the processes that are undertaken by legal expert systems are based on workflow systems. This means that the provision of this part of the service to the client comes at a significantly decreased cost.

Susskind gives the example of the insurance industry, where there is automation of high volume, low value tasks and activities. This way of automating workflow can enhance the efficiency of legal work to the point where, using a web-based service with the legal expert system available to the client on a 24-hour basis, the lawyer can literally make money while asleep.

The systemised approach can be applied to document drafting (an example of an automated document drafting system may be found at Automnio which is based on process flows – see https://autom.io/). Document automation requires users to answer a series of questions on a screen and after completion of the online form a first draft is made available. In none of this process has a lawyer been involved, unless the user inputting the necessary information is a lawyer.

This technology is not new. It has been around since the 1980s and it is a legal expert system in that it uses a rule-based decision tree. Susskind then takes the use of these commoditised systems a step further. If the drafting of certain types of contracts can be done online using a web-based interface, could this not be done within a client organisation? Why employ an expensive lawyer to draft "bespoke" standard form employment contracts, when the process could be undertaken within the human resources department of the organisation?

Does this mean that the lawyer gets cut out of the loop? Not necessarily. Susskind suggests that the lawyer "externalise" the service. "This occurs when lawyers pre-package and make their experience available to clients on an online basis," he says.

This is a different way of obtaining the expertise possessed by lawyers and presents a number of different or alternative business models. The externalised service can be made available as a chargeable one, albeit at a rate less than for the bespoke product. There may be advantages to a "per use" charging model at a rate that encourages reuse of the system. It may well be that it could be made available at no cost – a model favoured by government and charitable organisations such as law clinics. Alternatively, it could be made available on a "commons" basis in the spirit of the open source movement.

The advantages for the client are clear. The cost of legal services comes down. The price of those services – freed from the tyranny of the hourly rate – becomes more certain. The time to complete the work reduces. The quality of the output increases, because sitting behind the system is the collective expertise of a number of professionals which outclasses that of the individual.

Further reading:

- *John Zeleznikow and Dan Hunter "Building Intelligent Legal Information Systems in the Law", H.W.K. Kasperson et al. eds., Kluwer Computer Law Series 13 1994;*
- *Richard Susskind,* Tomorrow's Lawyers, 2nd Edition *(Oxford, 2017);*
- *https://autom.io/ (last accessed 6 July 2017).*

ADLS EVENT

Northland Lawyers' Lunch

ADLS invites practitioners in the Northland region to come along to the Northland Lawyers' Lunch at The Quay Restaurant in Whangarei on Tuesday 29 August 2017.

The ADLS Lawyers' Lunch Series provides a great opportunity to meet and network with fellow practitioners in your local area and provide feedback to ADLS on ways in which we can further support you in your professional career.

We hope you can join us at this event. The lunch will be $30.00 (incl. GST) from a set menu including a tea, coffee or juice and we are pleased to offer ADLS members an exclusive rate of $25.00 (incl. GST).

Time & date: 12.30pm, Tuesday 29 August 2017

Venue: The Quay, 31 Quayside, Whangarei

Registration: $21.74 + GST ($25.00 incl. GST) per person for ADLS members;

$26.09 + GST ($30.00 incl. GST) per person for non-members.

Register now to secure your spot, subject to availability. Visit www.adls.org.nz to register and pay online; alternatively, contact adls.events@adls.org.nz or phone (09) 303 5287. ADLS' standard cancellation policy applies for this event.

The ADLS Northland Lawyers' Lunch is proudly sponsored by MAS.

WILLS/ESTATES AND TECHNOLOGY

The future of will writing and estate planning?

By Lincoln Watson, Managing Director, Kōwhiri

An exciting time is approaching for the private client teams of law firms. The wealthiest generation in our history is ageing and, over the next 20 years, will be transferring assets to the next generation – who are possibly the most dependent.

Lincoln Watson

In the past, a major milestone such as the passing of a parent or loved one in someone's life has triggered an update to his or her estate plans. The fact that lawyers have this kind of a holistic overview on most facets of a client's life has given the legal industry a unique edge – the ability for lawyers to position themselves as trusted advisors. Every major event in a client's life provides an opportunity for the lawyer to discuss the client's future and suggest appropriate services that may be of value. By remaining in regular contact with clients, lawyers build a greater understanding of their needs and ensure that they are there for them.

What does the advent of the digital age mean for this area of law? For a start, we have seen consumer purchasing behaviour change significantly. New Zealanders now conduct in-depth research at the touch of a screen, and appreciate the flexibility and agency to make personal decisions alone. The "trusted adviser" model is breaking down with a move towards a more "modular" approach – where consumers seek out information and are happy to cherry-pick services from different providers if the service is convenient and provides value.

These changing approaches are having an impact in the private client practice area in particular, with potential clients increasingly looking to conduct their own research and consider ways of protecting their estates digitally. Research by New Zealand-based legal technology firm Kōwhiri has shown that at least 30% of people prefer to educate themselves online as opposed to meeting with a legal professional.

What questions might this raise for law firms? One option to consider might be partnering with a software provider to enable them to educate their clients online, thus adding value to the legal services they offer. Such an option offers the innovation of a specialist digital agency without the need to invest in the cost of building a bespoke system.

Software companies and digital agencies are positioning themselves online with flexible digital services and there are benefits to incorporating software into an estate planning model. When delivering services digitally, it is easier for law firms to focus on what they do well – assisting clients to address the issues and events that arise in their lives. Thomson Reuters recently conducted studies on law firms that had adopted document drafting software. It found that clients who manually drafted documents spent an average of 2.39 times longer on this process than law firms which had adopted document drafting software. Despite these sorts of findings, on average, only 4.7% of legal industry revenue is spent on IT services.

Making the most of available digital services may be pivotal to the success of firms which offer estate planning services, and may help to prevent them from losing ground to more progressive firms. But should law firms build their own systems from scratch or partner with a legal technology provider to stay in the game?

Kōwhiri's approach has been to tackle the question in collaboration with the legal profession, resulting in the development of "Arken", a new document drafting platform/intelligent will-writing software service that has been created by lawyers for lawyers and which will be launching here later this year. To ensure the clauses produced by Arken deliver the quality law firms expect, Kōwhiri is working with leading solicitor Greg Kelly. Arken will help lawyers produce high-quality estate planning documents at scale, ensuring all clients get a will that truly reflects their circumstances.

Kōwhiri is a legal technology firm based in New Zealand, providing Cloud-based document generation services that help private client lawyers draft wills and EPAs. Its software is used to create around 550,000 documents a year, across England and Wales, South Africa, Australia and New Zealand. For more information, visit https://www.kowhiri.com or https://arken.legal/nz.

WILL INQUIRIES LawNews

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

Email to: reception@adls.org.nz
Post to: ADLS
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 ADLS 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.

Maureen Anne BRADDOCK, Late of 23 Sunningdale Street, Manurewa, Auckland, Aged 75 (Died 26'05'2017)

Karla Eloise Victoria CLAPHAM, Late of Jaemont Avenue, Te Atatu South, Auckland, Aged 35 (Died 02'08'2017)

Peter Christian GOSCHE, Late of 85 Sir George Road, Avondale, Married, Aged 62 (Died 04'06'2016)

John Robert Woodward GRENVILLE, Late of 9B Peet Avenue, Royal Oak, Auckland, Widower, Electrical Mechanic, Aged 80 (Died 27'02'2017)

Vijay KUMAR, Late of 1/17 Luke Street, Otahuhu, Auckland, Aged 68 (Died 25'06'2017)

Siaosi Kenitini LELENOA, Late of 27 Sunnymead Road, Glen Innes, Auckland, Church Minister, Aged 48 (Died 08'07'2017)

Lance Dion NGAMOTU, Late of 162 Fitzherbert Avenue, Palmerston North, Aged 51 (Died between 18'05'2017 and 19'05'2017)

Jim SETO, Late of Henderson, Auckland, Retired, Aged 75 (Died 25'02'2014)

Paul Lawrence WILLIAMS, Late of 101 Bradbury Road, Howick, Auckland, Married, Retired, Aged 70 (Died 22'07'2017)

ADLS CPD

strata community association (NZ)

ADLS/SCA(NZ) Unit Titles/Bodies Corporate

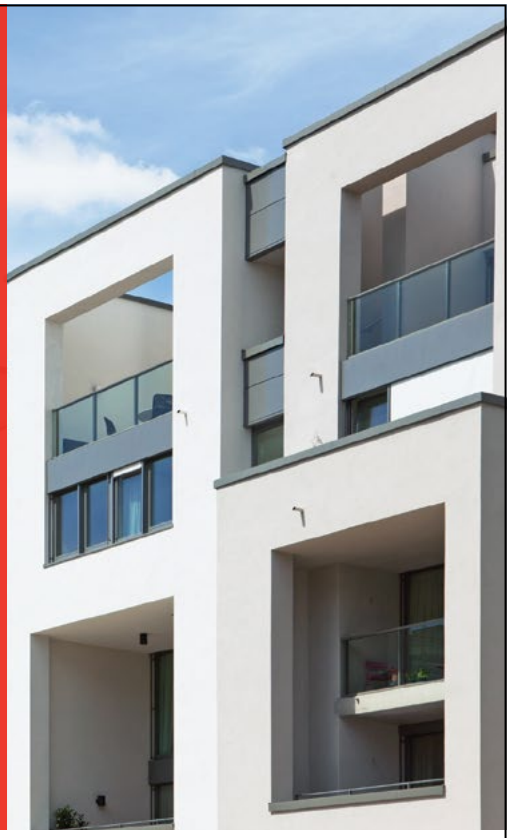
Half-Day Conference | 4 CPD Hours

Thursday, 21 September 2017
12:30pm - 5:00pm
Ellerslie Events Centre, Auckland.

Also available via live stream.

Early bird rate ends 8 September 2017.

For more information, pricing and to register please visit: adls.org.nz/cpd



ADLS members and non-member lawyers who have registered their Airpoints™ membership with ADLS can earn Airpoints Dollars™ on eligible ADLS CPD purchases.

ADLS Connecting New Zealand Lawyers | airpoints™

WANTED

Work experience opportunities

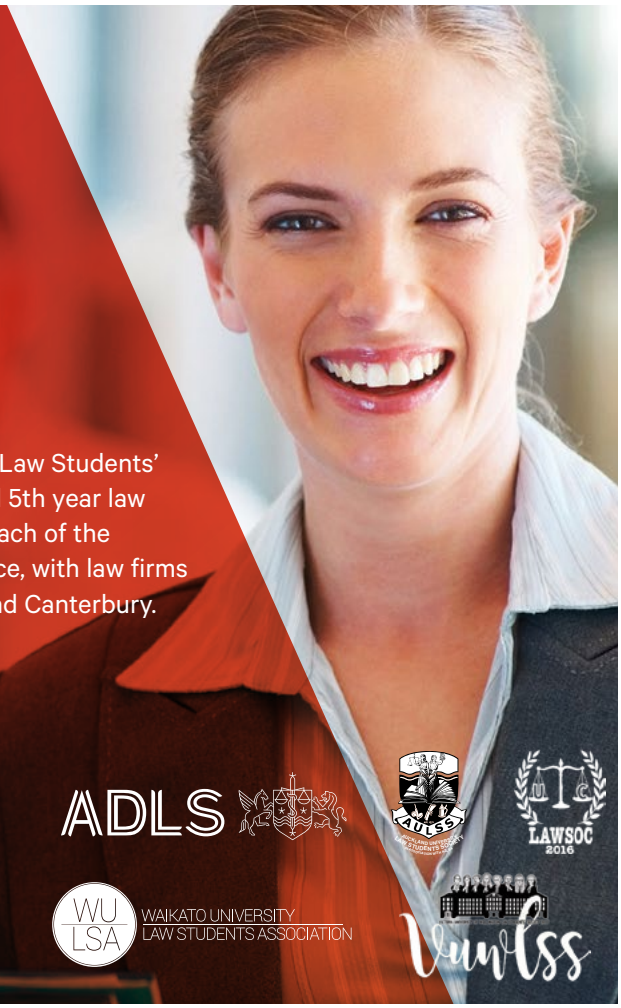
for 4th and 5th year law students

ADLS, in association with a number of New Zealand University Law Students' Societies, is running a Work Experience programme for 4th and 5th year law students. The programme aims to connect law students from each of the Universities seeking part-time paid or volunteer work experience, with law firms offering such opportunities in Auckland, Waikato, Wellington and Canterbury.

The programme provides law firms with an opportunity to work with those students they may select, to help the firm with tasks that may require some additional assistance. It also gives students valuable experience of how a law firm operates.

If you or your firm is able to offer a part-time paid or volunteer work experience opportunity to a 4th or 5th year law student, you can post the details free of charge on the ADLS noticeboard at www.adls.org.nz. For more information on the work experience programme, please contact ADLS on (09) 303 5270 or email workexperience@adls.org.nz

Terms and conditions apply, for full details please visit adls.org.nz



ADLS

AULSS

LAWSOC 2016

WU LSA WAIKATO UNIVERSITY LAW STUDENTS ASSOCIATION

VUWLSS