THIS WEEK'S ARTICLES

Issue 30
30 Aug 2019

ADLS
Connecting New Zealand Lawyers

LawNews

adls.org.nz

LAW & TECHNOLOGY

How new technologies are reshaping the law

By Rob O'Neill

Media regularly produce lists of the jobs most and least likely to be automated by robotics and artificial intelligence, but not many of these feature the legal profession.

That could be about to change.

MinterEllisonRuddWatts has deployed an AI tool in the form of a Microsoft Word plug-in that it helped fund. The tool, AuthorDocs, uses neuro-linguistic programming and machine learning to speed and improve the laborious contract review process.

At the global launch of the product in Auckland last week, the tool's New Zealand developer McCarthyFinch indicated it was preparing several more technologies for rollout, some of which could have a more direct impact on jobs than AuthorDocs.

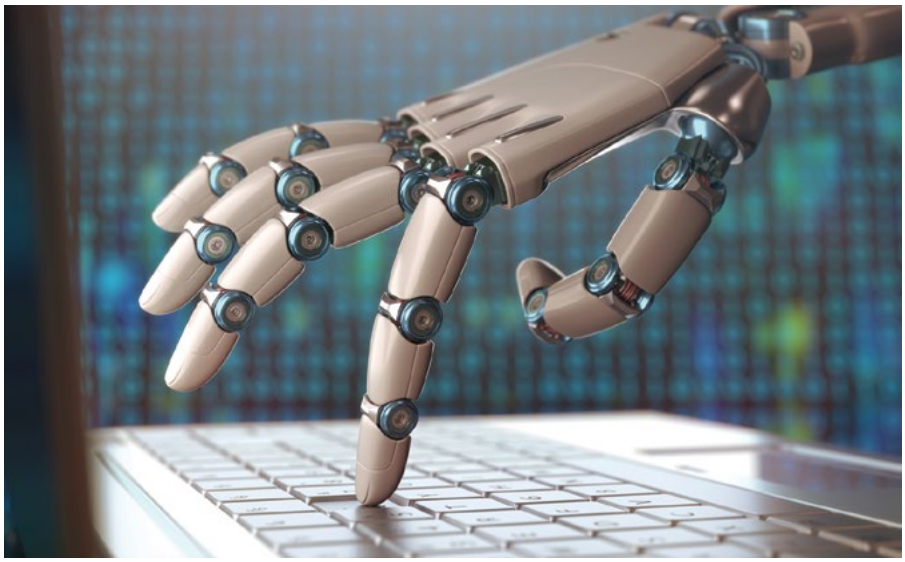
It seems intuitive that it will be a long time before a robot can carry a complex argument in court or design creative new business structures.

But then you might once have argued that robots could not deliver empathy and human engagement, something being fast disproved by avatar technologies from the likes of New Zealand's own Soul Machines.

Investment in legal tech platforms reached US$1 billion last year across 40 identified deals, according to a report by analysts Tracxn Technologies. Of that, US$362 million was invested into legal software using AI.

The tasks most suited to automation with current commercial AI are those involving repetition or research with high levels of accuracy, said Josh Comrie, the founder of New Zealand conversational intelligence technology developer Ambit AI.

The legal profession has many such functions, from research to conveyancing and document preparation and checking.



© Kts | Dreamstime.com

It's too early to tell whether artificial intelligence will revolutionise the practice of law

In a test of a daily legal risk assessment task, human lawyers achieved an average performance accuracy rating of 85%, while the average AI tool was 94% .... the average time human lawyers required to complete the process was 92 minutes while the AI system turned out its results in 26 seconds

Welcome to the **sixth** annual special Technology & Law edition, put together by ADLS' Technology & Law committee.

"Many of these tasks are far better suited to either a process or an algorithm," Comrie said. "In my opinion, the holy grail for law is a detailed and actual cognitive insight into what a client wants to achieve and then how to go about representing this in some form of outcome.

"While this may eventually occur, the real, realisable current benefit for the profession is in removing the low-level heavy lifting of junior solicitors."

This, however, would pose a long-term challenge to

Continued on page 2

How new technologies are reshaping the law

Continued from page 1

the profession; that is the kind of work experience that produces senior lawyers.

The development of AI and robotics offers opportunities as well as threats.

Digitally-progressive law firms can prosper by developing and deploying technology to disrupt their own businesses and the industry through improved efficiency and accuracy as well as automation.

As with other industries and professions, the jobs – or, perhaps more accurately, the "tasks" – that will fall to the robots first will be very specific.

The legal discovery process, for example, is already being boosted by smart technologies such as natural language processing.

But some early tests are showing robots can achieve better consistency and accuracy than humans in relatively complex tasks, especially when a lot of written material needs to be processed.

Last February, legal automation company LawGeex released a report comparing the performance of 20 experienced United Nations lawyers to its AI system.

Other automation technologies such as document management are likely to have as big an impact on legal operations as AI in the short term

"Few would be surprised that artificial intelligence works faster than lawyers on certain noncore legal tasks," the report said. "However, lawyers and the public generally believe machines cannot match human intellect for accuracy in daily fundamental legal work."

In a test of a daily legal risk assessment task performed on contracts from the Enron dataset, however, human lawyers achieved an average performance accuracy rating of 85%, while the average of AI tool was 94%.

The real, realisable current benefit for the profession is in removing the low-level heavy lifting of junior solicitors

Almost as pertinent, the average time human lawyers required to complete the process was 92 minutes, while the AI system turned out its results in 26 seconds.

Perhaps the most notable thing about this test and several others is that it did not focus on mundane tasks or commoditised legal work, but on the core function of legal advice.

The core technology used was proprietary legal language processing (LLP) and understanding models that learn "legalese".

"The LLP technology allows the algorithm to identify these concepts even if they were worded in ways never seen before," the report explained.

Lowndes Jordan partner and technology law specialist Rick Shera also said it would likely be the low-hanging fruit – commoditised, easily-repeatable tasks – that will be impacted first.

Strategy work such as anticipating the other side's responses and positions are much less likely to be automated.

"Those are decisions that humans will have to make and may never be replaced by AI," Shera said.

Tasks such as trademark applications can be automated through database integration. The intellectual property office, IPONZ, has already rolled out a beta tool allowing people to make their own inquiries about desired trademarks.

As with any new technology, AI adoption could be slowed because it is always a challenge to move people to new ways of working, Shera said.

However, even law firms that don't outwardly adopt AI could find themselves using it because many of the profession's software vendors are starting to build it into their products by way of upgrade. AI, for instance, is already embedded and being widely (if largely invisibly) used as part of common email and other desktop tools.

That could mean most businesses won't actually have control of their own AI technologies, Shera said, potentially raising more concerns and trust issues about who has access to, and use of, personal and confidential data.

Shera said other automation technologies such as document management are likely to have as big an impact on legal operations as AI in the short term.

At the launch of AuthorDocs, MinterEllisonRuddWatts CEO Andrew Poole said after investing more than $1 million in the company and a huge amount of time, he believed the tool would deliver immediate benefits to all lawyers, but particularly in-house lawyers and those in private practice, enabling them to work smarter and faster while focusing on quality.

Digitally-progressive law firms can prosper by developing and deploying technology to disrupt their own businesses and the industry

"Our firm had a choice about whether we would be disrupted or be part of that disruption and we are much happier to be part of the disruption," Poole said.

"We recognise that change is coming. We're not quite sure what the magnitude of that change will be in legal services, but there is no doubt change is coming."

Poole said as well as wanting to service clients

Continued on page 6

LawNews

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

Editor:
Jenni McManus

Publisher:
ADLS

Editorial and contributor enquiries to:
Jenni McManus, phone 021 971 598
or email jenni.mcmanus@adls.org.nz

Advertising enquiries to:
Jenni McManus, phone 021 971 598
or email jenni.mcmanus@adls.org.nz

All mail 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 $140 (plus GST) per year. To subscribe, please email reception@adls.org.nz.

LAW & TECHNOLOGY

Protecting your clients from cyber attack

By Edwin Lim & Lisa Paz

Are we *really* still banging on about cybersecurity? Well, yes - but hear us out.

In a world where data is more valuable than oil, and cybercrime supposedly generates more revenue than the entire global drug trade, it's unsurprising that cyberattacks are occurring on an unprecedented scale.

New Zealand is not immune. CERT NZ (the Computer Emergency Response Team) was set up by the government in 2017 as a one-stop-shop to receive cyber incident reports, track cyber incidents and provide advice on how to respond to an attack.

Between January and March 2019, CERT NZ received 992 cybersecurity incident reports, including the highest number of 'unauthorised access' incidents ever received. These incidents caused $1.7 million in direct financial loss to the individuals and businesses impacted.

Why should you care?
As lawyers, our duty to protect data is greater than that of most other businesses.

Firstly, we hold highly-sensitive and valuable commercial information about our clients, making us prime targets for hackers and scammers.

Secondly, our duties as members of the profession and as fiduciaries to our clients extend to implementing appropriate cybersecurity measures.

In today's climate, our strict confidentiality obligations and duty to take reasonable steps to prevent crime or fraud being perpetrated through our practice naturally extend to taking reasonable steps to ensure the security of our electronic systems, client and employee data.

Clients are increasingly aware of the importance of cybersecurity and want assurances that all appropriate measures are in place.

It is common for both new and existing clients to require law firms to complete cybersecurity questionnaires to clarify how sensitive client information is protected, with the answers forming part of the overall assessment of whether to engage or to continue to engage a firm.

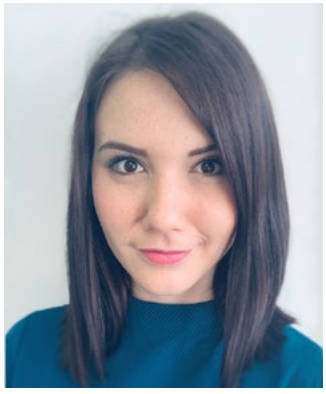
Key questions
As service providers to our clients, firms need to be able to articulate:

- what cybersecurity measures are in place to proactively protect information within its control;
- what IT functions are being outsourced and to whom;
- whether information security deficiencies are identified, reported, and tracked to resolution;
- how frequently security patches are applied;
- what user access management practices are employed and how – for example, is access granted only where required for the job function? Is access approved by the system owner? How often is employee access reviewed?
- what relevant training its staff receive;
- whether data is encrypted. If so, how?
- how the firm is continuously improving its cyber-security; and
- how the firm would detect and respond to a cyber attack.

Some clients may also require legal advisors to sign service provider agreements that contain significant obligations around data security.

The concern is understandable. Law firms are a hacker's paradise; an internet search for the phrase "law firm hacked" returns an alarming number of results (and what's just as bad is the number of law firms that don't even know they have been hacked).

Edwin Lim



Lisa Paz

As guardians of valuable client information, we are required to take cybersecurity seriously

Not only are hackers rewarded with access to information about multiple businesses at once, but they also get the juiciest information about those businesses - including information on top secret, and potentially market-influencing, deals, new IP, legal advice and information about disputes and settlements.

Unsurprisingly, law firms overseas are increasingly being targeted. The most famous example is the hack of offshore law firm Mossack Fonseca's poorly-protected email server which resulted in 11.5 million confidential documents being leaked in what became known as the Panama Papers.

But even a smaller-scale cyber-attack or scam could be devastating to your business, with enormous potential for financial, business and reputational damage.

Obligations around cybersecurity also rest on company directors. The Institute of Directors has confirmed the board's fiduciary duty of care to protect the company's assets includes protecting information and other digital assets.

We, as in-house or external legal counsel, need to ensure company directors are aware of this obligation. It's not good enough for directors to simply say they did not know about cybersecurity.

The writing is now clearly on the wall. Cybersecurity is no longer just an IT issue. It's a business issue.

Once a "nice to have", law firms can no longer ignore having advanced cyber security in place (actually, having anything in place is a good start!).

As guardians of valuable client information, we are required to take cyber security seriously. If your policies and procedures haven't been revised in a while, now is the time to dust them off and put appropriate measures in place to protect your clients and your business. It's as simple as that.

Edwin Lim is a partner at Hudson Gavin Martin, a commercial and corporate law firm specialising in technology, media and IP. Lisa Paz is a senior solicitor at Hudson Gavin Martin.

LAW & TECHNOLOGY

Is the cloud right for your firm and your clients?

By Richard Anstice

The IT industry loves a good buzzword.

At the moment, it's all 'in the cloud'. At the same time, law firms are looking to upgrade their IT, which includes moving to online-based services. So, what key issues should they consider?

The term "cloud" identifies a range of services where a business buys the use of fast, modern computers located in a service provider's premises and operated by the service provider.

The whole point of 'cloud' is that the customer doesn't have to buy new servers; instead, customers buy the use of services month-by-month.

"Public cloud" refers to larger suppliers who usually (but not always) deliver services to NZ from computers located in Australia. Big names are Amazon Web Services, Microsoft Azure and Google. There are lots of options to scale up and scale down the services you use.

For law firms, a key consideration about moving to the public cloud is that data is stored overseas, usually in Australia, so it is subject to the jurisdiction of Australian courts.

It is also subject to some espionage-related Australian legislation that means cloud providers may be required to access data without telling you. All law firms need to think about who their clients are and decide whether these risks are acceptable for the firm.

"Private cloud" refers to a range of services hosted on a smaller scale in NZ.

A key feature of private cloud is that the service can be highly customised compared with the generic offerings of public cloud suppliers. There are some great Kiwi firms offering quality NZ-based solutions.

"On-premises" is the current buzzword for having your own computer servers hosted in your own offices – aka "the old-fashioned way".

All servers storing the firm's data should be encrypted, either in the cloud or on-premises. If the encryption works as it should, the encrypted data can be decoded only by using an encryption key – a unique string of letters and numbers. The law firm can decide who controls the encryption key:

- If the law firm holds its own encryption key, it has the best control. But if the firm loses the encryption key, then it loses access to its data.
- The law firm can appoint a NZ IT firm to act as its agent to hold the encryption key. This means even if data is stored in the public cloud in Australia, the company holding the encryption key is in NZ, subject to NZ law. This makes it harder for foreign law enforcement agencies to access the firm's data.
- If ease of use is the priority, the cloud provider can manage the encryption key.

The cloud isn't always the solution – for example, some firms have clients who are too vulnerable to interference from foreign governments.

To make the right decision, a firm needs to have a frank discussion.

Off-site providers can offer better physical security for computers. Cloud providers have strong incentives to keep all servers up-to-date and properly patched for security. Cloud systems are set to back-up automatically, without needing to remember tapes or hard drives.

Using the cloud gives law firms access to some amazing technology. It helps firms to work remotely, connect with clients and manage documents. It's worth looking past the buzzwords to see what is there for your firm.

Richard Anstice is legal counsel for Fujitsu New Zealand

LAW & TECHNOLOGY

'Digitally excluded' lack access to essential services

By Conor Masila

Those of us working in offices or studying at university are attached to technology, allowing us not only to connect with friends and family but also to access essential services such as internet banking, IRD and Study Link.

The ability to navigate a world where the pace of technological change is accelerating must be learned, and many New Zealanders are not benefitting from, or able to participate in, the digital world.

These people lack basic digital skills or cannot access the internet reliably. Digital exclusion is an impediment when it comes to accessing essential services and in terms of their access to justice.

The term includes those who lack access either to the internet or a device, or the skills, ability, confidence, or finances to effectively use the internet.

The pace of technological change is significantly altering the way the government operates and the way it interacts with consumers.

What, for example, are the implications of moves towards online government and justice services? Any technological development in these areas should improve access to essential services and the courts, rather than making it harder for those already on the wrong side of the digital divide.

Conor Masila

Unequal access to justice and government services undermines equality in society, particularly as disadvantaged and vulnerable groups disproportionally experience legal hardship and therefore have a higher use of such services.

Moving government and justice services online may reduce access to justice for those who lack access to, and the skills to use, technology.

The government has set out an action plan on how it plans to address the digital divide in New Zealand.

The Digital Inclusion Blueprint was the first stage in the Digital Inclusion Action Plan and this year the government aims to identify priority areas and test small-scale initiatives.

During 2020 and 2021 the action plan expects to review digital inclusion goals and priorities, and check that these are still relevant.

The blueprint will be used to coordinate various government and community initiatives, and to identify where future investment will be needed.

Efforts to realise digital inclusion need to be evidence-based and to solve people's problems in ways that are proven to work.

Innovative thinking, a focus on user needs and continued learning from users' experiences will be crucial in preventing digital exclusion from being a feature of modernising government and justice services.

Solutions must look beyond implementing new networks and wifi access services. Instead, it will be important to evaluate socioeconomic conditions, education and the knowledge and skills needed to use any proposed technology.

Conor Masila is an Equal Justice Project representative

LAW & TECHNOLOGY

Does New Zealand need a specific law for deepfakes?

By Antonia Modkova

Have you seen the video where Elon Musk declares he is running for US president, that Tesla will start making flying cars and his new start-up will experiment on his own brain?

While you might be forgiven for believing Musk might say those things, the video is actually a deepfake fabricated by Hao Li, one of the fathers of deepfake technology, to warn of the dangers of his creation.

Deepfakes are hyper-realistic audio and/or video depictions of individuals which are, in fact, fake. While they appear to represent real events that have been captured by a microphone or camera, they are artificially constructed from existing photos, videos, and recordings by means of "deep learning" artificial intelligence (AI).

Just as photoshop enables photos to be manipulated, deepfake technology allows video and audio to be created depicting people doing and saying things they never did or said.

It has been possible to create fake media for a while but only recently has the technology become more generally available.

Exacerbating this accessibility is the huge amount of data now freely available online from which deepfakes can be generated. This includes data about public figures mined from media coverage, as well as data about private individuals extracted from their social media accounts and personal blogs.

Legal remedies

A law foundation-commissioned report *Perception Inception: Preparing for deepfakes and the synthetic media of tomorrow* recently examined the extent to which New Zealand law is equipped to address harmful misuse of deepfake technology.

Here is a glimpse of how New Zealand law might already regulate certain uses of deepfakes.

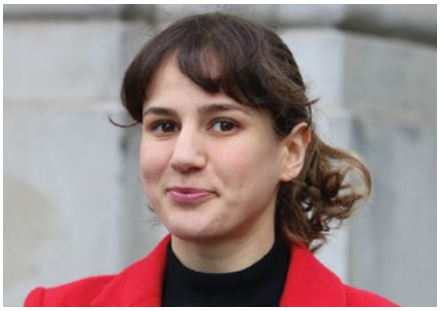
Deepfakes threatening privacy and emotional wellbeing.

Privacy law is an obvious candidate for protecting against unauthorised creations of deepfakes of individuals as it is directed to protecting an individual's ability to control their personal information.

However, while a deepfake might look real, the events it depicts might never have happened. So how can it be "personal information"?

Interpretation of the Privacy 1993 Act suggests false information about identifiable individuals, including fictitious depictions, may still qualify as personal information; otherwise provisions about rights to correct information would be meaningless.

Therefore the report's authors conclude deepfakes should be regarded as personal information because they are "information [that purports to be] about an identifiable individual".



Antonia Modkova

Another issue: a person's face and voice is generally public information.

Assuming deepfakes are synthesised using only publicly-available footage, how can they disclose any private information?

The authors of the report posit that the deepfake itself cannot be public information because it purports to depict events which never happened and were not "public" until the deepfake was created and published.

It will be interesting to see how privacy law evolves in this area. Does someone have a reasonable expectation that deepfakes will not be created? And would deepfakes be considered offensive to a reasonable and ordinary person?

Other statutes providing remedies against harmful deployments of deepfakes include:

- The Defamation Act 1992. Does a deepfake harm an individual's reputation?
- The Harmful Digital Communications Act 2015. Does a deepfake cause "serious emotional distress"?
- The Harassment Act 1997. Has the deepfake been used for harassment? The broad wording of the Act means intentional appropriation of someone's likeness in a way that causes distress is likely to be covered.

Committing crimes

Lying and deceiving are not illegal in their own right but s 240 of the Crimes Act 1961 criminalises obtaining, or causing loss by deception, any property, privilege, service, pecuniary advantage or benefit.

This extends to using deepfakes to illegally obtain or cause loss – for example, by impersonating another by using a deepfake. Threatening to create or disclose a deepfake for blackmail is also criminalised by s 237 of the Act.

Uses of deepfakes to induce or incite certain actions, whether by deception or blackmail, are criminalised in relation to slavery (s 98), sexual exploitation (s 98AA), murder (s 174) and suicide (s 179).

As the Crimes Act covers attempted crimes, even the use of blatantly unconvincing deepfakes can be criminalised.

The criminalisation of "revenge porn" using deepfakes under s 216G remains an open question. Section 216G criminalises intimate visual recordings made without consent.

But a sexually-explicit video of a person can be created using deepfake technology without any intimate visual recording of the victim being made – for example, by transplanting a victim's face onto another person's body where explicit footage of the other person's body may have been captured with full consent.

Misinformation and fake news

The Fair Trading Act 1986 (FTA) is likely to apply to misleading or deceptive uses of deepfakes "in trade" (s 9 to s 12).

"Unfair trade" is broadly defined to encompass any unfair conduct, regardless of its form. Section 13 of the FTA also prevents the unauthorised use of someone's image or identity to imply sponsorship, approval, endorsement or affiliation with advertised goods or services.

New Zealand law gives some protection against using deepfakes to spread fake news through legsiation such as the Defamation Act, the Broadcasting Act and the Electoral Act.

A public figure who has been misrepresented using a deepfake has recourse under the Defamation Act. Traditional defences to defamation such as truth and honest opinion might be unsustainable where the deepfake is a construction purporting to depict a real event.

The Broadcasting Act 1989 protects use of deepfakes in radio and television; however it is limited when it comes to the internet.

Section 197 of the Electoral Act 1993 (interfering with or influencing voters) and s 199a (publishing false statements to influence voters) may be of some assistance against use of deepfakes to interfere with the democratic process but they ar restricted in their application.

Given their rapid onset and potential harm, some countries have jumped to propose deepfake-specific laws. Does New Zealand need to follow suit?

The conclusion of the law foundation report was "probably not" as our law is drafted in a broad and media-neutral manner.

Law restricting deepfakes should be handled with extreme caution because, like all other audio-visual information, they are protected under freedom of expression legislation.

As the report suggests, nuanced amendments to existing law where there are gaps is preferable.

Antonia Modkova is a computer scientist, lawyer and patent attorney, specialising in AI and the management of the intellectual property portfolio of Soul Machines

Hate speech law: be careful what you wish for

By Andrew Easterbrook

Should our hate speech laws be expanded to include discrimination in areas such as gender, sexuality, religion or disability?

The goal is worthy. A concern underpinning the review of existing hate speech law, with its focus on racial discrimination, is that it may be inadequate to protect minorities and the disadvantaged from abusive and harmful speech.

But it is important to remember hate speech laws and policies have often been used to oppress and target minorities, rather than protect them.

The current discussion seems to be coalescing around whether sections 61, 63 and 131 of the Human Rights Act 1993 should be expanded.

Section 61 prohibits the dissemination of words "likely to excite hostility against or bring into contempt" people on the ground of their colour, race or ethnic or national origins.

Section 63 prohibits the use of language or behaviour that expresses hostility, if it is hurtful or offensive, and if it has a detrimental effect on a person in relation to specified areas, including employment applications, qualification, access to goods or services and education.

Broadly speaking, racist speech is unlawful if it is likely to incite hostility or contempt, or if it actually expresses such hostility or contempt and has a detrimental effect on a person.

The drafting is limited to racial discrimination. Several commentators have noted it does not cover discrimination (or "hate speech") on the basis of gender, sexuality, religion or disability. Some suggest those grounds should be considered for inclusion into the Human Rights Act.

When questioned about the review, Justice Minister Andrew Little told newsroom.co.nz, "The whole notion of freedom of speech and the protection of freedom of speech was always conceived of as a protection of the powerless against the powerful and we shouldn't forget that."

Andrew Easterbrook

Addressing harmful speech is tricky. It requires nuance and awareness of context

Lessons might be learned from the policies of social media giants such as Facebook and Twitter.

Those companies have generally taken a prescriptive and strict approach to content they say they will allow on their platforms. So they provide a visible and useful example of how broad hate speech rules might be drafted and how they might play out in practice.

Both sites' policies include broad prohibitions on hate speech and bullying.

But implementing those policies often goes awry. For example, Facebook banned the activist Celeste Liddle four times for violating community standards with her posts about a comedy show featuring topless Aboriginal women.

Wired magazine pointed out the alarmingly high frequency of LGBTQ activists being blocked by Facebook after using reclaimed terms such as "dyke".

And the very mechanisms designed to allow the reporting of offensive content can be abused by bad actors.

Katie Notopoulous had her Twitter account locked after the alt-right mass-reported an old tweet. In late 2018, trans activists noticed an increase in suspensions for their use of the word TERF (an acronym representing anti-trans feminists), tied to a mass-reporting campaign.

Addressing harmful speech is tricky.

It requires nuance and awareness of context which might vary from region to region. And it also requires an alertness to the fact that rules and reporting systems and legal institutions can be abused by bad actors to cause more harm.

The review should be approached with these lessons in mind.

The Harmful Digital Communications Act 2015 seems to have struck a reasonably good balance: few civil proceedings are brought under that Act. Instead, most complaints are dealt with quickly and efficiently by Netsafe, which tries to avoid re-victimisation.

Similarly, the Human Rights Tribunal has a broad discretion to dismiss proceedings if they are trivial, frivolous, vexatious or are not brought in good faith.

In this way it stopped Graham McCready's "private prosecution" against Sir John Key ([2015] NZHRRT 48).

But it still took six months and a 22-page decision for that to happen. The system should be better than that. Not everybody has the former Prime Minister's resources or stamina.

Andrew Easterbrook is an associate at WRMK Lawyers

Continued from page 2

better and see a return on its investment, the firm wanted to be part of AI to understand it and not to be a bystander.

"We don't know whether AI is going to revolutionise the practice of law. Some people say it will. But certainly this tool, if not revolutionising it will certainly be of huge benefit to lawyers as a whole."

James Schellhase, CEO of McCarthyFinch, said AuthorDocs was designed for every day, not heavy-projects use, within Microsoft Word "where lawyers work" and where engagement with the client also happens.

AuthorDocs was built to deliver "time to value" and requires no training, he said, but it was also a gateway product before McCarthyFinch progresses into the more advanced AI solutions it would soon be offering.

These include a contract approval and workflow automation product, another automating the drafting of contracts, and yet another that extracts key information from masses of documents.

McCarthyFinch is far from alone in its efforts. AI is breaking out all over.

Many of these tools are those lawyers can use rather than tools designed to replace lawyers.

Canada-based Blue J Legal, for instance, is developing an AI system that can help tax professionals gauge the strength of their legal position by applying AI to previous judicial decisions and findings.

That said, it seems likely in the medium to longer term fewer lawyers will be required as a result of AI, especially at entry level and in areas with repetitive, lower-level work.

Rob O'Neill is a freelance journalist specialising in technology

LAW, TECHNOLOGY & PRIVACY

Lessons for Kiwi companies in huge data breach fines

By Frith Tweedie

The past 18 months has seen unprecedented global attention on privacy issues. And a recent spate of huge fines shows privacy regulators are not afraid to flex their muscles when it comes to requiring businesses to take their privacy law obligations seriously.

The Cambridge Analytics scandal erupted in early 2018, demonstrating how our data can be "weaponised" against us and the risks posed to basic democratic processes.

That was followed in May by the introduction of Europe's game-changing General Data Protection Regulation (GDPR). Combining the threat of fines of up to €20 million, or 4% of annual global annual turnover – whichever is higher – with its extra-territorial effect, the GDPR has encouraged both individuals and organisations around the world to pay attention to privacy and data protection issues.

Cost of violations

Fifteen months on from the enactment of GDPR, European data protection regulators are hitting their stride.

In January 2019, the French privacy regulator fined Google €50 million (NZ$86 million) under GDPR for transparency and consent violations in relation to use of personal data in personalised ads.

The regulator's decision gives a clear message to all organisations collecting personal data online that information as to data processing practices must not be "described in a too generic and vague manner". The decision also emphasised that regulators are prepared to enforce GDPR's notoriously onerous consent requirements.

Two recently-announced GDPR fines dwarf even the Google sanctions. They also demonstrate that GDPR risks are not the exclusive preserve of big technology companies, signalling the need for both robust security practices and the inclusion of privacy law considerations in M&A due diligence.

On 8 July 2019, the ICO (Information Commissioner's Office) issued a notice of its intention to fine British Airways £183 million (NZ $346 million) for poor security arrangements that resulted in British Airways' website traffic being diverted to a fraudulent website. The personal information of approximately 500,0000 individuals was compromised, including log in, payment card and travel booking details.

Information Commissioner Elizabeth Denham said, "the law is clear – when you are entrusted with personal data you must look after it. Those that don't will face scrutiny from my office to check they have taken appropriate steps to protect fundamental privacy rights".

Frith Tweedie

The Equifax settlement, one of the largest in US history, affects approximately 147 million people or almost 50% of the US population

Only a day later, the ICO issued a further notice of its intention to fine US-based Marriott International Inc £99 million (NZ$187 million) for GDPR violations as a result of a data breach at the Starwood hotels group in 2014. Although not discovered until 2018, the cyber incident occurred two years before Starwood was acquired by Marriott in 2016 and involved the exposure of 339 million guest records, including those of 30 million EU residents.

The ICO's investigation found Marriot "failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems".

It emphasised the importance of "carrying out proper due diligence when making a corporate acquisition and putting in place proper accountability measures to assess not only what personal data has been acquired but also how it is protected. Personal data has a real value so organisations have a legal duty to ensure its security, just like they would do with any other asset. If that doesn't happen, we will not hesitate to take strong action when necessary to protect the rights of the public."

Privacy sanctions

The US Federal Trade Commission (FTC) formally announced its staggering US$5 billion settlement with Facebook on 24 July 2019, following its investigation into the Cambridge Analytica scandal. The FTC had charged Facebook with eight separate privacy-related violations, including that the company made deceptive claims about consumers' ability to control the privacy of their personal data.

As well as the record-breaking and "history-making" $5 billion payment, Facebook has agreed to an order that, among other things, prohibits it from making misrepresentations about the privacy or security of consumers' information and the extent to which it shares personal data. Facebook is also required to implement a reasonable privacy program.

The Facebook FTC fine came only days after Equifax agreed to pay at least US$575 million – and potentially up to US$700 million – as part of a settlement with the FTC, the US Consumer Financial Protection Bureau and 50 US states and territories.

That settlement stems from Equifax's 2017 data breach, one of the largest in US history, affecting approximately 147 million people or almost 50% of the US population. According to the complaint, "hackers were able to access a staggering amount of data because Equifax failed to implement basic security measures," including storing passwords and network credentials in plaintext.

New era

What does this mean for New Zealand?

The fines, combined with a seemingly insatiable media appetite for privacy breach stories, have put privacy issues squarely in the spotlight.

While falling well short of introducing the comprehensive privacy protections of GDPR or even the California Consumer Privacy Act 2018, New Zealand's Privacy Bill will summon a new era of transparency through the introduction of mandatory reporting of privacy breaches next year.

If the international experience is anything to go by, New Zealand is likely to see a significant uplift in reported data breaches once the changes become law.

And the implications for Kiwi businesses with such lax security that they are not prepared to address, manage or notify a data breach are significant and extend well beyond the bottom line. While the maximum fine of $10,000 barely registers alongside the GDPR and FTC fines, the collateral damage to an affected company's reputation is likely to be significant once damaging stories hit the headlines.

If data is the new oil, then data breaches are the new oil spills. New Zealand organisations would be well advised to pay attention to the growing regulator, consumer and investor focus on privacy, understand their obligations and act now.

Frith Tweedie is the digital law leader at EY Law New Zealand

Tread warily with changes to copyright law

By Melanie Johnson

New Zealand has a once-in-a-lifetime opportunity to rethink copyright, enabling it to take full advantage of technological innovation.

But the discussion tends to provoke exaggerated claims and misinformation on both sides of the debate.

The complexity of copyright law and its application to almost every aspect of our lives makes unpicking the truth difficult.

In the age of sound bites and fake news, catchy phrases such as "free use is not fair" and "user rights take money out of authors' pockets" are readily understood.

Lawyers' professional expertise in unpicking the facts and interpreting the law creates an obligation to ensure these myths and exaggerations are debunked if we are to craft legislation that supports innovation and technological change.

The Minister of Commerce initiated the formal review of the Copyright Act by setting out the issues to be considered: "The vast reach of copyright – and the rapid pace of technological change today – makes it critical to ensure that our copyright regime is working the way it should: to enhance our collective social, cultural and economic well-being."

Given its importance, we need to evaluate carefully all claims calling for changes to the Act.

The copyright regime worldwide has progressively enacted provisions which benefit rights owners and limit user rights.

As the Australian Productivity Commission observed in its 2017 report on IP, Australia's copyright arrangements are skewed too far in favour of copyright owners to the detriment of consumers and intermediate users.

Rights owners have used several tactics to convince legislators that as advances in technology have enabled the man in the street to copy and share the creative works of others with relative ease, the rights of users should be limited.

One such tactic has been to focus on the diminished earnings of creators.

The *Writers' Earnings in New Zealand* report was commissioned by Copyright Licensing New Zealand in conjunction with authors and playwrights.

Writers who took part in the research earned around $15,200 a year from their writing. NZ Society of Authors noted: "It is timely to ponder this sum...in light of the review of the Copyright Act.

"Authors forgo considerable income through lack of compensation for the exceptions we already have in law."

Melanie Johnson

Such statements create a smoke-screen that obscures the identities of the real beneficiaries of any tightening of copyright law.

The return creators are receiving has diminished but not because the term of copyright is too short or users' rights too permissive.

Reports from the UK and the US show book and music sales have increased although this increase is not necessarily matched with publisher income.

Several reasons have been put forward for this, including that technology has enabled platforms such as Amazon, with its global reach, to push the price of books down.

The continuing demise of profits for musicians has been attributed to intermediaries becoming involved and taking excessive chunks of the earnings.

Copyright academic and researcher Professor Rebecca Giblin argues claims that copyright has affected authors' earnings miss the point.

These claims are motivated by good intentions – most notably "the desire to sustain writers' incomes in an era of precipitous, disastrous decline .... In the UK, earnings of professional writers have dropped 42% in real terms between 2005 and 2017."

The government's issues paper makes the point that "copyright does not guarantee that creators will make money from the economic and moral rights they have in their creative works".

It provides them with only the opportunity to negotiate payment in return for authorising others (by licensing or transferring copyright) to use their work (eg, make copies available to the public).

As Giblin has observed, the parties are free to bargain and some publishers have extracted every right to every payment, worldwide, forever, leaving the author with zero entitlement to future royalties, or any licensing fees that might be paid

This explains how such a big share of copyright's rewards can end up being transferred to others.

Claims by rights-holder groups not only risk unbalancing copyright, they also prevent scrutiny of publishing practices impacting on writers' incomes.

This is not to say changes shouldn't be made to the Act to improve authors' incomes.

Solutions should be considered such as the recent EU copyright directive which introduced an obligation to force publishers to be more transparent when reporting information to authors about the exploitation of their works and the revenues generated.

The directive also included 'bestseller' clauses and rights to fair remuneration.

The US and the EU have included in their legislation rights reversion clauses so, rather than leaving it to individual contracts, rights are returned to authors after a certain time, opening new revenue streams for authors.

The primary rationale for copyright is to incentivise the creation of works, increasing access to information and culture.

The longer term for copyright has done the opposite and has restricted the availability of books.

Giblin, along with colleagues Jacob Flynn and Francois Petitjean, tested copyright's 'underuse theory' across New Zealand and Canada, which have a 50-year-plus life term for copyright, and Australia and the United States, which both have a 70-year-plus life term.

By investigating the relative availability of ebooks to public libraries, they found books are less available where they are under copyright than where they are in the public domain.

The research found that books from 59% of the 'culturally valuable' authors sampled were unavailable in any jurisdiction, regardless of copyright status.

This provides new evidence of how even the shortest copyright terms can outlast works' commercial value, even where cultural value remains.

They also found works were priced much higher where they are under copyright than where they are in the public domain, and these differences typically far exceed what would be paid to authors or their heirs.

Melanie Johnson is legal counsel at the University of Auckland, advising on copyright and licensing

LAW & TECHNOLOGY

The challenges to blocking 'bad' content online

By James Ting-Edwards

With the internet now reaching four billion people, consumers and policy makers are focusing on the ways it can be used for good or ill.

In the wake of the Christchurch mosque killings and the livestreaming of the attack and related documents on website 8chan, the conversation is about how we can best protect our communities against the worst ways people use the internet.

As part of their immediate crisis response, New Zealand's major internet service providers (ISPs) used blunt technology tools to block their customers from 8chan and other websites hosting this content.

We are now seeing discussion about the longer-term role of local ISPs in preventing access to dangerous content online. My goal in this article is to offer some of the technical and policy context needed for a useful policy conversation on those issues.

Whether it be through a fibre line or a cellphone tower, your ISP connects you to the internet, allowing you to request and receive the data packets that enable email, web browsing, online banking, and everything else online.

While there is only one global internet, it is made up of cooperating parts. We can compare it to a city, where the underlying infrastructure of streets, water pipes, and buildings enables people to come together, do business and live their lives.

For the internet, the core of that underlying infrastructure is the protocols and technologies that enable connections between computer networks built and operated by different people in different places around the world.

To connect you to that broader infrastructure, your ISP must build or buy access to the data you need, whether by hosting computers in a data centre or by buying access to international submarine cables or satellites.

For a normal user, most of this technical complexity is hidden. You can take it for granted that internet packets will turn up in the same way we typically take it for granted that office buildings will have power, running water and postal services.

But the details of that technical complexity are vital when considering policy measures to address online content.

There are some inherent challenges with measures to block online content. Blocking measures tend to be either too strong (resulting in unintended interference with legitimate use of the internet), too weak (failing to block access by motivated people) or both.

ISPs blocked 8chan as part of their crisis response

James Ting-Edwards

While ISPs have some technical tools to control New Zealanders' access to online content, that is not their role

by interfering with the normal way users accessed domain names.

Domain names are a human-readable type of address on the internet. A website like that of the Auckland District Law Society typically has a domain name like "adls.org.nz". By typing in that address, or clicking a link to it, people can tell their devices to look up the relevant online server and access content from it.

Most users rely on the default service offered by their ISP for domain name lookup. So, by stopping the normal way a domain name lookup works, an ISP can stop users with the default configuration from looking up a domain name.

This approach has a few downsides.

Firstly, it is easily avoided by motivated people. Internet users can choose to use an alternative provider of domain name lookups, which will not be affected.

Second, it can block only at the level of a whole domain or website. Much of the concerning distribution of material from the Christchurch attacks took place through popular platforms such as Facebook. Though there were serious issues at stake, blocking New Zealanders' Facebook access does not seem like a proportional response and would not make ISPs popular.

The most important point is about who should make these decisions and how.

Under the New Zealand Bill of Rights Act 1990, New Zealanders have the free expression right to "seek, receive, and impart information of any kind in any form".

The internet and the use of platforms such as Facebook is clearly an important way New Zealanders exercise this right. How do we navigate the tension between protecting this free expression right and effectively addressing the serious issues raised by the Christchurch attacks?

I do not have the answer but can suggest a potential direction.

Under section 5 of the Bill of Rights Act, the rights affirmed can be subject to limitations that are demonstrably justifiable in a free and democratic society. Our courts have interpreted this in terms of legality, necessity, and proportionality.

In other words, limitations on free expression and other rights should be imposed only under the law, and those laws should be crafted to ensure impacts on rights are necessary to achieve an important purpose, and are proportional to the importance of that purpose.

We await a royal commission report to tell us in detail how the Christchurch attacks could have happened. In the meantime, we can think carefully about options.

While ISPs have some technical tools to control New Zealanders' access to online content, that is not their role.

Blocking measures tend to be either too strong (resulting in unintended interference with legitimate use of the internet), too weak (failing to block access by motivated people) or both

As the ISPs themselves have said, we need a public conversation to develop a legal framework for this. My suggestion would be that our existing framework under the Bill of Rights Act is a useful starting point for discussion and for deciding what impacts and benefits are justified to serve important policy purposes.

James Ting-Edwards is senior policy adviser at Internet NZ

Why two-factor authentication isn't secure

By Lloyd Gallagher

Two-factor authentication (2FA), an extra layer of protection beyond a user name and password, has been heralded as a saviour for data protection in an increasingly-insecure online world.

But how secure is it really? And are there potential legal issues for corporate clients?

In our opinion, 2FA is not secure and clients may face increased liability as legislators and the public begin to realise the assumptions they have been operating under for 2FA security are incorrect.

Law firms should refrain from using 2FA as an authentication mechanism and move to MFA (multi-factor authentication) options, or other timed key authentication mechanisms.

Advice to clients running internet businesses requiring logins should be to steer away from 2FA in favour of more secure mechanisms to reduce the risk of data breach.

The risks of using 2FA will only increase as hackers become more savvy.

Extra authentication

The purpose of 2FA is to secure parties' access by adding a second layer of authentication through an alternative method based on real-time processing, such as email or SMS messaging.

The methodology requires simplicity, while adding separation to a simple login and password authentication.

Both email and SMS operate in a similar fashion, with the request executed by the webserver's login script executing a second script. This generates a unique code that is then sent to the device you choose when activating the 2FA system.

This security addition appeared plausible to most users. However, both email and SMS have similar flaws when transmitting secure data to the receiving device.

This article will not focus on email, save to say that email is subject to spoofing through simple techniques and lacks encryption mechanisms.

Instead I will focus on SMS (simple messaging services) and why 2FA is also insecure on SMS mechanisms.

SMS is considered secure because it is believed to be a carrier delivery network that runs on its own separate platforms.

But it operates over the internet due to the low cost of delivery compared to ISDN (integrated services digital network) and other network delivery systems. These are no longer attractive to carriers and have been largely abandoned.

Lloyd Gallagher

In spite of the Peer-2-Peer design of SMPP, it is still vulnerable to the same security hacking as email and other insecure platforms

Many also assume that because the carriers use the internet, it must have a level of security in its deployment. This is simply incorrect.

SMS suffers the same flaws as email with lack of security.

Origins of SMS

SMS was developed in late 1992 as a mechanism to transfer data using agreed topology through the telephone networks.

Its initial development was based around mobile phone implementation. In late 2007, to standardise the industry transmission information, SMPP (short message peer-to-peer) was launched.

This quickly became the dominant SMS delivery service and is still used because of its reliability, standardisation, ease of deployment and backwards compatibility with older carrier networks.

However, SMPP is not deployed with any form of security because many carrier systems run on the aforementioned older hardware were developed before security became a major concern. It is here that the trouble for 2FA begins.

Carrier of choice

Due to the standardisation needed to delivery SMS reliably worldwide, SMPP is the main, and arguably the only, choice for carrier SMS delivery.

Despite advances to add TLS (transport layer security), many older systems will not be replaced, leaving the SMS insecurities in play for years to come.

In spite of the peer-to-peer design of SMPP, it is still vulnerable to the same security hacking as email and other insecure platforms.

With the increased use of unregistered VoIP (voice over internet protocol) operators, and in spite of the use of http (non-secure web protocol) and https (secure web-based protocol) which are deployed via APIs (application programming interfaces) by many non-carrier VoIP operators, SMS is still largely delivered via SMPP even where it originates in https platforms, leaving 2FA delivery vulnerable to attack.

One example saw hackers develop a VoIP carrier network that allowed customers to port numbers into their service.

Then in late 2018 the operator snooped the SMS message sent and received one customer's VoIP numbers, including the 2FA requests. This was then used to access the customer's information on various sites to obtain data.

This is just one example of many stories involving 2FA breaches that are coming to light with the increased use of 2FA as companies become more concerned with internet security.

A warning

As with email, techniques such as phishing, malware intercept, social engineering, man-in-the-middle and website proxies are all risk factors with 2FA security. The National Institute of Standards and Technology (NIST) in 2016 issued a warning:

Due to the risk that SMS messages may be intercepted or redirected, implementers of new systems should carefully consider alternative authenticators. If the out-of-band verification is to be made using an SMS message on a public mobile telephone network, the verifier shall verify that the pre-registered telephone number being used is actually associated with a mobile network and not with a VoIP (or other software-based) service.

SMS 2FA is still the most-used mechanism in the world to secure login access, with companies arguing that the NIST statements are only a recommendation and not meant to be taken literally.

But who holds the legal liability for data loss? In most cases firms bypass responsibility and liability as the public operates under the misunderstanding that 2FA creates security.

This is not the case. As the security concerns on 2FA become better-known, it is likely firms will see increased liability where 2FA is deployed and data loss occurs.

Lloyd Gallagher is a director of Gallagher & Co and convenor of the ADLS Technology & Law committee

ADLS EVENT

ADLS dinner with the Minister of Immigration

On Thursday 8 August, the Immigration and Refugee Law Committee hosted Immigration Minister Iain Lees-Galloway at the Northern Club. The annual dinner was well attended by many members of the bar and professionals from the immigration sector.

Committee convenor Deborah Manning presented the committee's comprehensive 10-year review of the Immigration Act 2009 to the minister.

The review is intended to highlight deficiencies in the legislation and suggest areas for improvement, particularly around increasing access to justice in the immigration and refugee context. It also notes New Zealand's recent vote to adopt the Global Compact for Safe, Orderly and Regular Migration provides a timely opportunity to review the Act and ensure it aligns with the government's expressed commitments.

The minister addressed attendees on the government's areas of focus for the next year and also took questions. There was lively discussion and a common theme was the progress made in the past year towards better engagement between MBIE (the Ministry of Business) and the immigration bar.

The committee thanked the minister for carrying through on his promise to drop Refugee Status Branch timeliness figures. This means the Refugee Status Branch should no longer feel compelled to set down interviews quickly, giving counsel and refugee claimants more time to prepare cases.

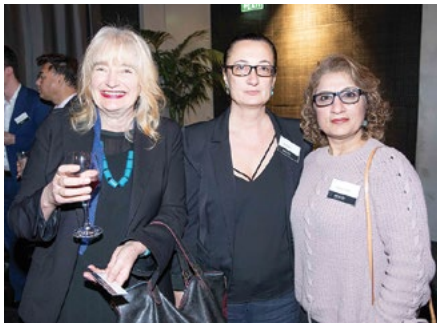
If you would like a copy of the Immigration and Refugee Law Committee's 10-year review of the Immigration Act 2009, please visit the Immigration and Refugee Law Committee page on the ADLS website: www.adls.org.nz/for-the-profession/committees/list-of-committees/immigration-refugee-law

Justice Matthew Palmer, Matthew Robson, Martin Treadwell and Immigration Minister Iain Lees-Galloway

Sam Parsons, Simon Lamain, Raj Singh and Joseph Tresidder

Immigration Minister Iain Lees-Galloway, ADLS Immigration & Refugee committee convenor Deborah Manning and Stewart Dalley

Ben Hansard, David Cooper and Lukas Sousa



Carole Curtis, Ioana Uca and Darsan Singh

ADLS EVENT

ADLS Breakfast with Attorney-General David Parker

ADLS invites the legal profession to its popular event, Breakfast with Attorney-General David Parker, on Friday 6 September.

Join us for a hot breakfast and an address from the Attorney-General, followed by a Q&A session.

Breakfast will be held at the Rydges Hotel's Rooftop Terrace, featuring a 360-degree view of the harbour.

Tickets are $50 for ADLS members and the judiciary, and $65 for non-members. If you would like to attend, please register now to avoid missing out.

Date & Time: Friday 6 September 2019, 7.15am – 8.30am

Venue: Rooftop Terrace, Rydges Hotel, 59 Federal Street, Auckland

Tickets: $50 for ADLS members and the judiciary*
$60 for non-members*
*All prices include a hot breakfast, non-alcoholic beverages and GST

RSVP: Register before Monday 2 September 2019 to secure your place, subject to availability. Visit www.adls.org.nz to register and pay online, alternatively contact events@adls.org.nz, or phone (09) 978 3970. *ADLS' standard cancellation policy applies for this event.*

Featured CPD

Iwi Settlements and Kaitiakitanga: Engaging with the $50bn Māori Economy – FINAL NOTICE

The Māori economy is now estimated at $50bn, but managing large investments comes with great responsibility. Māori-owned businesses are unique because they are driven not just by financial outcomes but by the principles of kaitiakitanga (responsibility), manaakitanga (supporting people) and taonga tuku ihi mō ngā uri whakatipu (guardianship of resources for future generations). What are the key legal and cultural factors you need to take into account when working with firms which do business with Māori entities? How do we ensure that Māori legal and financial structures meet their cultural and ethical responsibilities? How does the tax system work for and against iwi? The specialist Te Wake Ture team at Chapman Tripp will walk you through what you need to know.

Learning outcomes:

- Gain a deeper understanding of the post-settlement governance model.
- Learn more about how the tax system affects Māori.
- Learn the pros and cons of using limited partnerships.
- Gain insights into how to do business with Māori entities.

Seminar Livestream
CPD 2 hrs
Tue, 3 Sep
4pm – 6.15pm
Presenters
Te Aopare Dewes
Rōia Whakarae (Senior Associate)
Te Waka Ture, Chapman Tripp
Robert Grignon, Senior Legal Advisor, Tax, Chapman Tripp
Chair
Geoff Hardy, Partner,
Martelli McKegg

Trusts for Today

Many lawyers will have dealings with trusts whether acting as trustees, providing clients with advice or drafting trust deeds. Understanding trusts and keeping up to date with developments in trust law is therefore essential. This session will provide insights into trusts generally and what lawyers need to do to ensure existing and future trusts (in light of the new Trusts Act) are fit for purpose.

Learning outcomes:

- Learn more about the issues that may arise with existing trust deeds as a result of recent case law development, and how to use powers to vary and update trust documentation.
- Gain insights into the makeup of trustees, who the beneficiaries are, the need for unanimity and the implications of this for trustees.
- Understand better the requirements for the diversification of investments under s 13D of the Trustee Act 1956, and the problems that may arise from self-interest, self-dealing and conflicts of interest and how these may be affected by the Trusts Act.

Webinar
CPD 1 hr
Wed, 4 Sep
12pm – 1pm
Presenter
Tammy McLeod, Director,
Davenports Harbour Lawyers

Commercial Law Series: International Distribution Agreements

Taking a product to overseas markets might be an attractive proposition for a business client but it carries varied and multiple risks. There are numerous considerations such as freight, customs and jurisdiction; and country-specific factors to add to the matrix. This webinar will provide guidance on how your clients can safely and successfully sell their products to the world, and in turn offer you an opportunity to enhance your relationships with them.

Learning outcomes:

- Get a feel for the export landscape, including opportunities and resources available plus current trends.
- Become apprised of key considerations and the models available for distribution.
- Delve into the operational aspects of distribution of which you and your clients need to be aware, including channels, pricing, performance and exit.
- Receive a checklist of legal and operational matters in this area to assist you minimise your clients' risk and facilitate your own best practice.

Webinar
CPD 1.25 hrs
Thu, 5 Sep
12pm – 1.15pm
Presenters
Grant Dunn, Partner,
Buddle Findlay
Craig Armstrong, Customer Director – Auckland, NZTE

Successful Settlements: Making the Most of a Mediation Process

With mediation and other forms of alternative dispute resolution the norm for the disposal of most litigation in New Zealand, best practice requires that the lawyers acting be involved with making crucial decisions. This seminar aims to assist litigators with the ins and outs of the mediation process, from deciding whether to mediate to crafting the settlement agreement.

Learning outcomes:

- Receive guidance on the decision to mediate and, in turn, how to approach the choice of mediator.
- Become better informed about how to time the key consideration of entry into mediation.
- Gain insights into the multitude of factors required for preparing to negotiate from a mediator's perspective.
- Gain a better understanding of the role that insurance may play in this context.
- Become equipped with specifics of the items that should be detailed in an agreement, to provide certainty for those involved as much as possible.

Seminar Livestream
CPD 2 hrs
Thu, 12 Sep
4pm – 6.15pm
Presenters
Paul Dale QC
Warren Sowerby, Mediator
Cecily Brick, Partner,
Fee Langstone
Chair
The Honourable Rodney Hansen CNZM QC

CPD in Brief

Burning Issues in Employment Law Forum 2019

Forum
CPD 2 hrs
Thu, 19 Sep
4pm – 6pm

The conflagration of topics and scorching presenters that is the Burning Issues Forum is back; covering the searing issues of the moment it is too hot to miss. With its Royal Assent blistering the page, the Employment Relations (Triangular Amendment) Act is a firestorm waiting to be tackled. Domestic Violence – Victims Protection Act is aflame with uncertainty while the availability of workers after the *NZ Postal Workers* case is alight with implications for employment lawyers. Finally, as the hot embers glow and spark, there is the searingly hot question of penalties in light of *Preet*, *Prabh*, *Victoria 88* and *Nicholson*. Please note, because of the nature of this event, papers will not necessarily be provided.
Drinks and nibbles will be served following the forum.

Presenters: His Honour Judge Perkins; **Catherine Stewart**, Barrister; **Kylie Dunn**, Partner, Russell McVeagh; **David France**, Partner, Kiely Thompson Caisley

Chair: Catherine Stewart, Barrister

Your Legal Business: Working Flexibly – Making it Work from All Sides – JUST LISTED

Seminar
CPD 1.5 hrs
Tue, 24 Sep
4pm – 5.30pm

Flexible working seems here to stay – but what is it, why have it and how do you achieve it? This seminar will provide key insights, for all legal professionals.

Presenters: Trina Lincoln, Associate General Counsel – Construction, Housing New Zealand; **Kylie Mooney**, Chief Executive Officer, Meredith Connell; **Sarah Pilcher**, Principal, The Franchise Lawyer; **Paula Williams**, People and Culture Director, Simpson Grierson. **Chair:** Geoff Hardy, Partner, Martelli McKegg

Giving it Away Before Death: The Ins and Outs of Gifting

Webinar
CPD 1 hr
Wed, 25 Sep
12pm – 1pm

Gifting as an estate-planning tool or as a way of assisting children into the property market is increasingly common. This session will look first at what needs to be done to make a valid gift and issues such as the mental capacity to do so. It will also focus on how to deal with undue influence from family members wanting gifts made in their favour and issues that arise in respect of relationship property, the Family Protection Act 1955 and the Law Reform (Testamentary Promises) Act 1949. This webinar is based on the session on gifting at the Cradle to Grave™ Conference 2019.

Presenter: Alison Gilbert, Partner, Brookfields

Personal Effectiveness Workshop

Workshop
CPD 4 hrs
Thu, 17 Oct
9am – 1.15pm

Do you want to have more impact at work? This workshop will provide a range of personal effectiveness insights and tools to help increase your productivity and return-on-effort at work. It is facilitated by a leading high-performance consultant. Feedback from the August workshop included the following comments: "Super presentation", "Relevant, informative content" and "Engaging, practical, down to earth and relateable".
This is the final time this workshop will be held in 2019. Places are limited. Register now to avoid missing out.

Presenter: Tony Gardner, Managing Partner, Catapult Auckland

Navigating Defamation Law: Strategies and Recent Developments

Seminar Livestream
CPD 1.5 hrs
Thu, 21 Nov
4pm – 5.30pm

Defamation is a complex and constantly-developing area of law. With social media giving anyone an unprecedented platform to share their views, the last five years have seen a significant increase in defamation claims. How do you ensure that defamation claims are dealt with quickly and efficiently? What strategies can you use to ensure a good outcome outside of, or in, court? What are the critical issues in defamation and what does the future look like? This seminar will give you a comprehensive understanding of these and other key issues in defamation law.

Presenters: Justin Graham, Partner, Chapman Tripp; **Tom Cleary**, Senior Associate, Chapman Tripp

CPD Pricing

Delivery Method	Member	Non-Member
Webinar (1 hour)	$80 + GST	$115 + GST
Webinar (1.25 hour)	$90 + GST	$130 + GST
Seminar (2 hour in person)	$130 + GST	$185 + GST
Seminar (2 hour live stream)	$130 + GST	$185 + GST
On Demand (1 hour recording)	$90 + GST	$130 + GST
On Demand (2 hour recording)	$145 + GST	$205 + GST

CPD On Demand

Earn CPD hours by completing On Demand activities via your computer or smart device

visit: adls.org.nz/cpd

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

Terms and conditions apply.

Iwi Settlements and Kaitiakitanga: Engaging with the $50bn Māori Economy - Final Notice

Tuesday 3 September | 2 CPD hours | Seminar & Live stream

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

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.

Adrienne Jill FRASER, Late of 530 Pinnacle Hill Road, Bombay, Auckland, Married, Retired, Aged 80 (Died 03'08'19)

Faye Lynnette HUMPHREYS, Late of Orewa, Auckland, Married, Company Secretary, Aged 74 (Died 27'06'19)

Siale 'O Failoto Koula KOLOI, Late of 81 Ferguson Road, Otara, Auckland, Single, Construction Worker, Aged 22 (Died 04'05'19)

Charles Alfred PFEFFERLE, Late of Whare Aroha Hospital, Rotorua, Permanently Separated, Retired, Aged 72 (Died 11'12'98)

Mark John SIVITER, Late of 70 Bradbury Road, Botany Downs, Auckland, Married, Operations Manager, Aged 37 (Died 09/08/19)

ST THOMAS MORE DINNER 2019

We are honoured to have as this year's speaker, Kathryn Beck.

Kathryn is the Immediate Past President of NZLS. As well as her role as President, Kathryn has been closely involved with gender equality in the legal profession; NZ Rugby's Respect & Responsibility Review Panel and encouraging the legal profession's implementation of mental and physical health initiatives.

Members of the committee extend a cordial invitation to all lawyers and friends to this year's St Thomas More dinner to be held on Wednesday 16 October 2019 at the Northern Club, Auckland.

As is our usual practice, the dinner will be preceded by Mass to be celebrated in the Maclaurin Chapel at the University on Princes Street at 6:30pm.

Pre-dinner drinks will be served at the Northern Club from 7:15pm for dinner at 7:45pm. The ticket price of $120.00 covers pre-dinner drinks, dinner and wine.

Tickets are limited so you are requested to RSVP by completing the form below together with payment by cheque or direct credit immediately to avoid disappointment.

✂ ..... Detach here

By direct deposit to Dawson Harford Limited Trust Account; ASB 123109-0032560-02 and confirm by email to bernard.smith@dawsonharford.com the information set out on the slip below; OR

If paying by cheque please make it out to "Dawson Harford Limited Trust Account" and post to PO Box 106347, Auckland 1143 together with the information slip below.

Name: .....

Postal Address: .....

Email Address: .....

Name(s) of attendee(s):
Title Christian Name Surname

.....

.....

.....

LAW & TECHNOLOGY

Electronic signatures: get clear on the process

By Lloyd Gallagher

Rapid technological change not only alters the way we live but also changes the language we use.

For lawyers, an understanding of technical words in a legal context is critical.

For example, "electronic signatures" and "digital signatures" are two terms often used interchangeably. This is incorrect. In fact, they have very different meanings and it is essential that lawyers understand the distinction.

Electronic signature
This is any signature in electronic form – ie, not a paper-based, ink signature.

Examples are a scanned image of your ink signature, a mouse squiggle on a screen or a hand-signature created on a tablet using your finger or stylus, a signature at the bottom of your email, a typed name, a biometric hand-signature signed on a specialist signing hardware device, a video signature, a voice signature, a click in an "I agree" checkbox, or any other form of electronic medium to indicate acceptance of an agreement.

Digital signature
This is a subset of electronic signatures, as it is also in electronic form.

However, digital signatures go much further by providing security and trust services in the signature delivery.

When activating a digital signature, the signer is verified through authentication, the data is maintained on an integrity server for cross-checking and the signature is secured by encryption to prevent repudiation and modification in transit.

So, a digital signature can be considered an electronic signature but an electronic signature cannot be considered a digital signature. This is an important distinction when issues of validity and repudiation come into play.

Electronic signatures provide a better user experience as they can reflect normal ink signatures by using images that users can identify with. The downside: they can be copied or forged from one document to another and documents can be easily changed after signing without detection.

Electronic signatures can be repudiated as there is no verification of who actually signed the document.

The big advantage of digital signatures is that signed documents cannot be changed without detection and the person signing the document can be determined with a high degree of trust. Signers cannot repudiate their signatures.

The downside is that digital signatures are based on cryptographic codes so are not easily associated with normal ink signatures.

Finalising the signature also requires several steps.

Language is constantly evolving. Where technical language enters a non-technical environment, there is always risk that a layperson's understanding based on common usage might prevail.

The legal profession needs to maintain evidential standards for electronic signing so clients are appropriately protected.

ADLS SEMINAR

How to make the most of mediation

Mediations are an integral part of civil litigation, more often than not leading to a definitive outcome.

But the skills associated with a successful court practice are not necessarily the same as those needed for mediation.

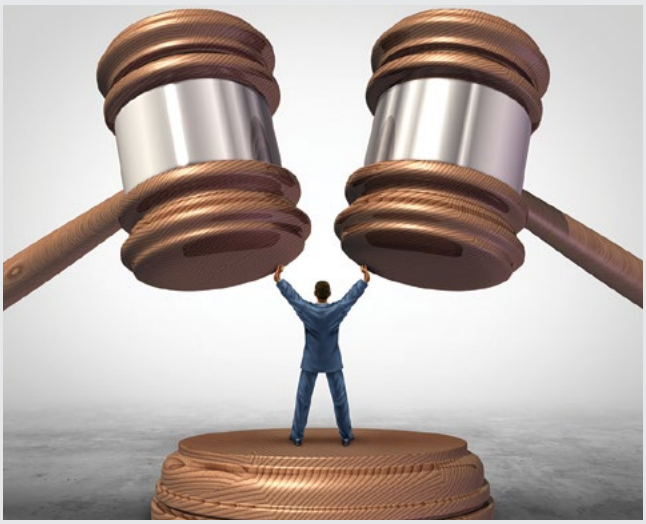
At an upcoming ADLS seminar ***Successful Settlements: Making the Most of a Mediation Process*** experienced mediators will explain why this is the case and teach you how to improve your mediation skills.

Achieving a settlement is one thing; achieving the best outcome is not necessarily the same.

Presented by Paul Dale QC, Warren Sowerby and Cecily Brick of Fee Langstone, and chaired by Rodney Hansen CNZM QC, the seminar will address ways of achieving good outcomes, and managing risk and avoiding common mistakes.

The issues will include:

- determining the point in the proceedings where a mediation should take place, along with the tactical considerations behind that decision;
- tactics around appointing a mediator and the role the mediator is expected to take.;
- protecting your client from the pressures leading up to a mediation and dealing with them in the context of the mediation itself;
- creative options and thinking outside the square; and
- how to stop a settlement from unravelling and drafting a settlement agreement to ensure it is full and final.



A settlement is not necessarily the same as achieving the best outcome

Because of the importance of mediation in the civil litigation context, all these issues confront practitioners at all levels.

Successful settlements: making the most of a mediation process will be held on Thursday 12 September. To register or for more information, visit www.adls.org.nz/cpd