THIS WEEK'S ARTICLES

Issue 29
24 Aug 2018

ADLS
Connecting New Zealand Lawyers

LawNews

adls.org.nz

Technology & Law
SPECIAL EDITION

LAW AND INFORMATION TECHNOLOGY

11 IT security issues that lawyers need to know about

By Arran Hunt, Principal, Virt Law

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

While we have IT support staff and services for a purpose, lawyers should still have a base understanding of the use of IT. However, many in the profession have picked up bad habits, or make poor assumptions about IT.

The list of IT security issues below may be a helpful starting point.

1. **Mobile phones, including SMS, are not a secure service**

Receiving a call or an SMS from a client's phone does not mean it came from that client. It is simple to fake someone's mobile number, and software like Skype has the ability built-in as a convenience. Always use a second method of confirming such information received.

And, while most lawyers would be unlikely to send important information by SMS, banks have created an unrealistic view of SMS security. For many bank customers, an SMS code is sent by the bank to confirm making an online bank transfer. However, the phone systems on which SMS operates are not secure. Devices (collectively called "stingrays") allow hackers to, amongst other features, collect any texts meant for the victim. The first devices of this type were released over a decade ago and, as with all technology, they have since developed and become more widely available. Fortunately, they are not simple devices to use, and for this reason we are not seeing many of them in use in New Zealand.

Continued on page 2

11 IT security issues that lawyers need to know about

Continued from page 1

However, some banks still seem to be oblivious to their existence. We have one client whose bank account was raided by a social hacker, who also appears to have used a stingray device to emulate our client's mobile number (and therefore receive the bank's security code SMS). We believe that several people, all located in the same town (all using the same mobile provider from the same cell tower) were hacked at about the same time, which would strongly suggest a stingray was used. When the bank was asked to comment on this security issue, it responded:

"We find it difficult to believe that this is possible or likely, nor have we been advised this is the case by #### [company redacted by article author] or other mobile phone network providers."

SMS is not a secure service and should not be treated as such. Law firms should use other methods to confirm bank transfers, and I would expect banks to be requiring this of any commercial client. In this situation, our client was not a commercial customer of the bank. We would encourage all clients to look at other methods to confirm bank transfers, such as the use of the dongles provided by banks to commercial clients.

2. Emails aren't secure, but they are probably still more secure than sending a letter

While every method of communication could be said to be insecure in some way, it is worth drawing particular attention to emails. There are multiple ways that they can be breached and used as an attack. Anything you receive by email that is of importance, such as a bank account number or instructions from a client, should be confirmed using another method.

For example, if the vendor's solicitor on a transaction sends you a bank account number, or a client emails to request a funds transfer from your trust account, call him or her to confirm. However, don't call on any phone number received by email, as that could be compromised as well.

3. Emails have a size limit

Emails have a size limit. It will typically be the lower of that set by the email provider of the sender, or that of the receiver (if the receiver's provider has a smaller size limit, then it should bounce back to the sender). These limits were put in place originally due to the slow speed of internet connections, where a 1MB file could take minutes to send or receive. Now that we can receive that same email in as fast as one hundredth of a second, such limits seem old-fashioned. Yet, the limits remain. This is not necessarily a bad thing, as emails aren't secure, so ideally shouldn't be used for sending such files. Online drop box services, with a code used to encrypt the files, are a better and more secure method.

Arran Hunt

As noted in point 11 below, emails may be counted as received if sent to a valid email address. For that reason, it is better for an email service to allow the largest email possible to be received, rather than you missing out on something which, strictly speaking, was correctly sent to a valid email address.

4. WiFi you don't control is not secure

At a recent event held at an Auckland conference centre, I asked how many of my colleagues had used the free WiFi to do work while at the event. Nearly every attendee raised a hand. However, none of them had encrypted that WiFi usage, despite not being able to confirm that the WiFi was properly secure.

All communication over a free WiFi service should be encrypted using a Virtual Private Network (VPN) service. These can be run by your firm or, more simply for most people, through a paid service. This will encrypt all information between your device and the VPN service, making your use of that WiFi service more difficult to monitor or intercept. While some may believe that WiFi at established centres can be trusted, as a user, you can't be certain that the staff at the facility have not tampered with the service, or that a hacker is not simply emulating that service (something that is very easy to do). The use of a VPN should be standard procedure for all mobiles and laptops when away from the office, unless you can be completely confident in the WiFi and network security.

5. Your own WiFi may be a security risk

If your firm gives WiFi access to clients or other visitors, then it should do so using a second WiFi service that does not have access to your local network. Otherwise, you are opening your network up to a third party. Many modern WiFi routers have this as a feature, so it can be done at relatively low cost.

6. Unused network ports in your office are a security risk

The same way that your office WiFi can be used to access your network, so too can any unused network ports in areas that non-staff can access, such as meeting rooms. Something placed in the way, such as a bag, could cover up someone's usage during a meeting, making you unaware of it.

Continued on page 3

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.

Continued from page 2

Any unused network ports should be disabled or, if they need to be available to staff, should be either in locked cupboards or in open sight with no way to use them without being seen.

7. Everything should be encrypted

It would take someone with basic IT hardware experience just minutes to disassemble a laptop and access the contents of its internal drive. All PCs, laptops, tablets and mobile devices should be encrypted, so they can only be accessed by someone who has logged onto the device. Most modern PCs and devices now include chips that make encryption relatively quick and unobtrusive. Windows 10 Pro should be encrypting by default. All firms should be certain that all of their devices, whether they are taken out of the office or not, are encrypted.

8. Remote delete

In the event that a device is lost, even password-enforced encryption may not be enough to stop someone accessing it, as security flaws for mobile devices are often found. For this reason, all mobile devices should have software installed allowing the firm to remotely delete the device. Such abilities are often built into the operating system (such as in more recent versions of Apple's IOS). Using this facility does usually require internet access. In the case of a mobile, it can sometimes be done by sending the phone an SMS with a pre-determined code. While not a perfect solution, it does help a firm protect a device that may contain, or have access to, client files, and allow for the device to be deleted before access can be gained. This rule should also be in place for any staff-owned devices that are used to access firm documents and/or emails.

9. Security begins in the office

While the media typically focuses on hackers, the easiest way for people to access your commercial files is to break a window and grab any paper copies. While it is important to consider the IT vulnerabilities, general security at the physical office should not be overlooked. This also covers any physical documents being taken home by staff.

10. Digital documents are easy to fake

While I am a strong advocate of the use of digital documents, they are as easy to fake as physical documents. Anything received digitally should be verified by another method. As in points 1 and 2 above, verify anything received through another method.

11. Check your spam folders regularly

With changes to the *Companies Act 1993*, and other statutes encouraging the use of technology, some communication is considered received on it being validly sent to a valid email address. If your spam filter has filtered it away from your regular email box, the liability falls on you, as it was validly sent to a valid email address. Knowing how spam filters work, it could also be possible for someone to send an email, tailoring it so that it is more likely to be filtered, not noticed, but validly sent. Therefore, your spam folder should be checked regularly. You should be able to scan through the list of senders and topics to quickly spot any that were incorrectly filtered. If an important email is filtered, remember to set your email software to handle emails from that sender correctly in the future.

These are not all of the issues that lawyers now face, but hopefully they will provide a basis to help you avoid some of the more common problems (ADLS regularly runs CPD events that can help you with these types of issues – keep an eye on adls.org.nz/cpd). Each firm should have at least one staff member who can act as the IT champion, educating the rest of the firm, and helping to put correct procedures in place. Ideally it should be someone who is familiar with law, so that the firm's responsibility as lawyers takes precedence over any preference of IT service providers.

TECH FOR LAWYERS

Review of PDF Split and Merge (PDFsam)

Reviewed by Arran Hunt, Principal, Virt Law

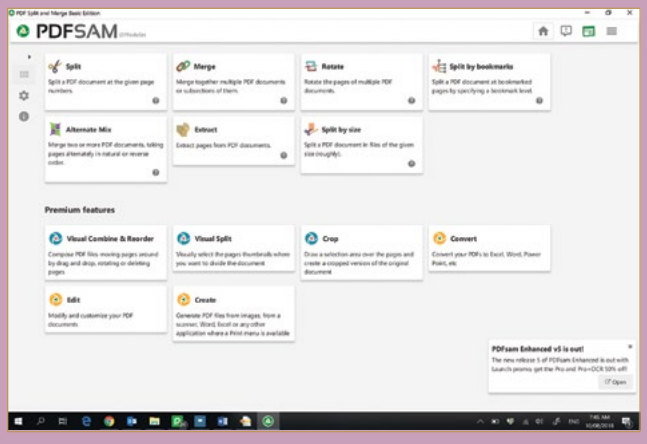
PDFs have long since become the standard document format used in law. They provide us with a simple way to send documents, at what is usually a relative small size. However, simple changes to how the documents are saved can be a hassle.

PDF Split and Merge (PDFsam) provides a simple way to do simple document manipulation. Using drag and drop controls, users can rotate documents, reorder pages, merge documents together, split a document into multiple parts, and make a number of file format changes. What can be especially useful is the ability to insert a page within a document, such as needing to insert a floorplan as an annexure to a contract. PDFsam provides all of this functionality and more.

Some of these services are also available online. However, such services require you to upload the document to a third party, something that would create a confidentiality issue. PDFsam operates on your local PC, so the documents remain within your control.

There is a free version, allowing users to try out most of the features. The full version can range from US$59 to US$99, although the highest priced product is currently discounted to US$49. The time taken to print, re-order, then rescan a document will already be more than the cost of the software, and the quality of the original document will be retained.

There is also a version with Optical Character Recognition (OCR). OCR is the recognition of a scanned document so that the text is identifiable. It allows you to scan a document, and then search for any term within that document, something that isn't typically possible (as the original scan was traditionally seen as an image rather than text). All firms should have at least one device or piece of software than can OCR a document,



especially when dealing with large documents or large amounts of printed communication.

PDFsam is software that I use perhaps once every two months, and have done so over the past several years. The benefits it provides far outweigh its small cost. It is simple to use, and would be useful to any firm that is handling PDF files.

https://pdfsam.org

COMMITTEE UPDATE

Introducing the ADLS Technology & Law Committee

Innovation lies at the heart of our changing world. From government policy to the practice of law, technology creates amazing opportunities and daunting challenges.

The ADLS Technology & Law Committee (Committee) sees itself as having a mandate to keep up-to-date with the times and offer relevant perspectives on topics such as modernising legal processes, privacy, intellectual property, online safety, cyber-crime and Cloud services governance.

The wider profession can occasionally struggle with the pace of technological developments and their impact upon law and legal practice. In this, its fifth annual special "Technology & Law" issue of *LawNews*, the Committee continues its focus on providing practitioners with articles and advice on new technologies.

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

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

Lloyd Gallagher (Convenor) is actively involved around the world in alternative dispute resolution where he acts as an arbitrator and mediator. With a strong IT background, he works with law practitioners and policy-makers to develop solutions that focus on access to justice and technology security. Mr Gallagher can be contacted at lloyd@gallagherandco.co.nz.

Richard Anstice has worked as a lawyer advising on a range of commercial transactions, including distribution and IT design and build, with a particular focus on the balance between the legal aspects of technology and the practical needs of non-technical people. He can be contacted at rdanstice@yahoo.co.nz.

Andrew Easterbrook works at Rob Harte Lawyer, dealing mainly with technology law, relationship property and estate litigation. He is a director and co-founder of openlaw.nz, an open legal data platform. He is also a musician and a computer geek. He can be contacted at andrew@hartelaw.nz.

His Honour Judge David Harvey was appointed as a District Court Judge in 1989, and sat at Manukau for 20 years, before transferring to Auckland in 2009. Judge Harvey was closely involved with information technology initiatives involving the judiciary. He was the director of the New Zealand Centre for ICT law at the University of Auckland Law School, until he was granted a temporary warrant and returned to the bench in April 2018.

Arran Hunt is the Principal at Virt Law. He previously worked as a technical business analyst, for a Fortune50 company in London and for several large firms and city councils in Auckland, before being admitted to practise law in 2010. He can be contacted at arran@virt.nz.

Melanie Johnson is legal counsel at the University of Auckland. She advises the University on a broad range of issues, including copyright, privacy and contracts, and 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 is a barrister and solicitor 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.

Getting technical with the ADLS Tech & Law Committee, pictured here holding its August meeting with remote participation

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

Edwin Lim is a partner at Hudson Gavin Martin, a boutique commercial and corporate law firm specialising in technology, media and IP. 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. Mr Lim is responsible for the IT infrastructure and roadmap at his 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 is a patent attorney and intellectual property lawyer at Soul Machines, a New Zealand R&D company developing hyper-realistic virtual humans. She holds conjoint degrees in law and science, and recently extended her technical expertise with an honours degree in computer science, focused on artificial intelligence and machine learning. She has a particular interest in legal issues arising from technological developments in artificial intelligence. She can be contacted at antonia.modkova@soulmachines.com.

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.

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

ARTIFICIAL INTELLIGENCE

How to cross examine an algorithm

By Antonia Modkova, patent attorney and intellectual property lawyer at Soul Machines

The legal system evolved to hold humans accountable for their actions. However, many of the actions that humans used to take are increasingly being performed by machines, thanks to the advent of machine learning. For example, algorithms are replacing or assisting humans in making decisions on creditworthiness, insurance, employment, education, and even sentencing.

Antonia Modkova

The myth of the black box

Machine learning algorithms are often called "black boxes", but it is actually very easy to lay out how they are programmed to make decisions in a general sense (after all, someone had to build them). It is even possible to unpack exactly how a certain input was processed in the algorithm to produce a certain output.

The problem is that, when we ask a human why they made a decision, we generally want to know abstract reasons or justifications for the outcome – not the inner workings of the brain mechanics which caused him or her to make the decision. Algorithms can make accurate predictions and decisions in a manner that is so complex and fundamentally unintuitive to humans (and lawyers!) that revealing their reasoning does not provide any useful insight. This is why roboticist Hod Lipson concluded that explaining how a complex algorithm made its decision can be as futile as "explaining Shakespeare to a dog". It's not that humans do not have access to the logic, rules or patterns – it's that we cannot follow that logic.

Nonetheless, there are several contexts in which use of machine learning algorithms can and should be legally scrutinised, without needing to understand the inner workings of the algorithm. Just as in human decision-making, with algorithms, there are significant variations in the role of explanation, who must provide the explanation, and what sort of explanation is required.

Discrimination

The requirement for explanation in alleged discrimination cases stems from our desire to protect certain groups from unfair treatment on the basis of illegitimate factors such as race, sex or religion. Key questions to ask engineers on the witness stand about this revolve around how input correlates to output, including:

- What were the main factors that affected the decision?
- Would changing a certain factor have changed a decision?
- Was a factor determinative?

The above questions are actually very easy to answer technically, and do not require a deep understanding of how the algorithm came to its decision. For example, it is easy to test if a factor was determinative – by removing it from the input and seeing how that affects the output. One thing to watch out for is that, even where potentially discriminatory factors are removed from the input, algorithms may still find a proxy for those factors (e.g. post code may serve as a proxy for race).

Liability

In March 2018, we saw the first fatal collision involving a fully-autonomous vehicle, being tested by Uber. Liability in such cases is still a grey area, but one might expect the focus to shift from negligence to product liability. However, what does it mean for an algorithm to be "defective"? Data scientists have a toolkit of metrics they can use to analyse the effectiveness of algorithms, including accuracy, precision and recall.

Alternatively, algorithms may be compared to what a human would have done in the same situation as the "golden standard". The fact that a computer program is 99.99% accurate might not save you in the 0.01% of cases when it fails – in fact it might not even be allowed as evidence. *Skounakis v Sotilly* (No. A-2403-15T2 (N.J. Super. Ct. App. Div. Mar. 19, 2018)) involved a death allegedly caused by a recommendation for a weight loss regime provided by a computer program. The defendant was unsuccessful in arguing that technical programming aspects are relevant to liability – only evidence from a physician was allowed.

Administrative decision-making

Where machine learning has been used to assist administrative decision-making, aspects to bear in mind are the legal doctrines of non-delegation, due process, transparency and discrimination. With respect to non-delegation, if an algorithm replaces a formerly human-made decision, the first question to ask is whether the decision-maker is even allowed to delegate the decision to a machine. Where an algorithm supports a human decision, the question then becomes whether the human exercised independent judgement or was he or she overly reliant on the algorithm? Due process and transparency require that machine learning algorithms and input data are readily available and provide the ability to scrutinise and meaningfully appeal a decision made by a machine.

The devil is in the data

It is important for lawyers to understand the different ways in which mistakes and unfair treatment can creep into machine learning algorithms.

Firstly, it is important to watch out for the use of inappropriate "training data". If training data is poor, the results will be poor. For example, if historical data was used to train an algorithm, human discrimination can be merely encoded by the algorithm and reinforced with each decision.

A second problem may be a lack of data. The accuracy of machine predictions generally depends on the amount of training data available. Even where a lot of training data was used, the algorithm may still fail when it comes to determining a case where there is under-representation of certain characteristics in the training data. In simple terms, an algorithm might not know what to do, because it has not seen many examples of that instance in the past.

A third aspect to be aware of is that algorithms can identify correlation but not causation. As the UK's Information Commissioner's Office explains, "where algorithmic decisions are made based on such patterns [in the data], there is a risk that they may be biased or inaccurate if there isn't actually any causality in the discovered associations".

The need for technological literacy

As more and more human activity is replaced by artificial intelligence, lawyers and judges need to be better equipped to understand and argue about machine learning. "Quantitative analysis" will be a skill that is highly valued in lawyers. Anyone can vaguely condemn what looks like discrimination or a mistake, but lawyers who understand the underlying technology will be far more effective. And you never know – it may come in useful when robots take over your legal work and you are forced to try to find work as a data scientist.

COPYRIGHT LAW, LAW REFORM

Copyright Act review – fostering innovation vs protecting owners' rights

By Melanie Johnson, Legal Counsel, University of Auckland

Do your clients find copyright frustrating? Are they concerned that an expansion of user rights could affect their earnings?

In June 2017, MBIE launched a review of the *Copyright Act 1994* (Act) to "ensure that our copyright regime is fit for purpose in the context of a rapidly changing technological environment".

Rights owners and user groups such as museums, libraries and educational institutions have met with MBIE to identify where greater protections may be needed, and where user rights should be expanded or updated to take advantage of technological changes.

The resulting issues paper (due for release in the fourth quarter of this year) will initiate the review process, including a 16-week public consultation period, and will provide the framework for assessing the copyright regime.

While analysing the submissions will take time, it will help Ministers make calls on the extent of the reforms. This may accelerate some changes or maintain the status quo, depending on the quality of the submissions. MBIE officials envisage the release of an options paper to test solutions sometime later in 2019 or early 2020.

Current regime

UK copyright law provided the model for New Zealand's law, and has the same sort of prescriptive fair dealing exceptions as Australia and a number of other former Commonwealth countries.

New Zealand has four fair dealing exceptions, the main ones being copying for the purposes of criticism and review, news reporting, and research or private study. New Zealand also has a number of other exceptions set out in Part 3 of the Act, including copying for education and for libraries and archives.

Prescriptive exceptions, while they provide certainty, do not readily adapt to developments in technology. For this reason, a number of countries (including Israel, Singapore, South Korea, Malaysia and the Philippines) have introduced a "fair use"-type exception for uses that fall outside the existing user provisions.

Other countries are also considering introducing fair use, including South Africa, which currently has a Bill before Parliament with a fair use clause. In Australia, the Australian Law Reform Commission and the Australian Productivity Commission have both recommended introducing a US-style fair use exception.

Melanie Johnson

In New Zealand, a number of submissions to the Select Committee on the Trans Pacific Partnership Agreement Amendment Bill called for the introduction of a fair use exception. Following this, InternetNZ released its "Getting Copyright Right in the Information Age" discussion paper in 2017, and Deloitte released "Copyright in the Digital Age" later the same year. Both recommended introducing a US-type fair use exception "to support innovation in a rapidly changing technological environment".

What is the difference between "fair use" and "fair dealing"?

The courts in the US establish fairness using a four-factor test, established by section 107 of their Copyright Act. This requires the court to consider the purpose and character of the new work, the nature of the copyrighted work, the amount and substantiality of the portion taken, and the effect the allegedly infringing work would have on the market.

The test for fairness in both fair use and fair dealing cases is similar, because both have common origins in UK case law. Does the use substitute for the work in the market and cause market harm to the rights owner? Copying books and songs instead of buying them is not fair. Other uses, such as copying a work of art or a segment from a film for review purposes, do not harm the market for the work. Both US law and the current New Zealand law protect such use of copyrighted works.

The difficulty with fair dealing is that it has a closed list of permitted purposes. Anything falling outside these purposes is infringing. It is the closed list which therefore differentiates fair dealing from fair use.

The fair dealing model in New Zealand creates a two-stage analysis: first, does the intended use qualify for one of the permitted purposes stated in the legislation; and secondly, does the use itself meet the fairness criteria?

Under the US system, any kind of use can be potentially fair, thus it offers far greater flexibility. The main benefit is that it enables technological innovation by permitting new fair uses of works not foreseen by the legislature.

The 1984 US case of *Sony v Universal Studios Inc* (called the "Magna Carta of the information technology industry"), demonstrates this. The court found that "time-shifting" a live recording to view it later was fair use. This decision was critical to encouraging the emerging consumer electronics industry, and has continued to provide businesses confidence to invest in developing innovative new technologies.

In contrast, VCR technology did not become legal until 1994 in New Zealand, and 2006 in Australia. Fair use futureproofs legislation in an environment of rapidly changing technology and enables products to be developed and manufactured without legislative clarification. Being first to the market is critical for many industries.

Why are rights owners concerned?

The recommendations of the Australian Law Reform Commission in 2014 and the Productivity Commission in 2017 met with strong opposition from copyright owners. The Australian Publishers Association, the Copyright Agency and APRA AMCOS, who represent the interests of copyright owners, are opposed to the introduction of a fair use exception.

The general concern is that a fair use exception to copyright infringement would be interpreted as allowing the free use of copyright material where that use should be paid for. Rights owners have also claimed that to introduce a fair use exception in Australia would stifle local creativity. This is despite the fact that the US courts have consistently held that a use cannot be fair if it affects a rights owner's market or the value of the work.

A similar response from rights owners has greeted any suggestion of fair use in New Zealand. The NZ Society of Authors equated fair use with the assumption "that it is fair game to use any and all content subject only to very minor limitations". Paula Browning, the CEO of Copyright Licensing New Zealand, reiterated a common concern that introducing fair use would create uncertainty about the law and result in increased litigation. "One of the benefits of the existing law and the certainty it provided was we don't go to court every five minutes." Ms Browning also rejected the suggestion that copyright laws were holding back innovation.

Is the opposition justified?

Research shows that the law in this area is well-

Continued on page 7

Continued from page 6

settled and that copyright litigation does not increase with the introduction of fair use. In the US, fair use rulings only account for 0.004% of all cases decided at trial level. As Bloomberg Law (reporting on litigation trends in the US) noted, a pornography company (Malibu Media LLC) brings most copyright litigation.

The Australian Productivity Commission gave little weight to a report commissioned by rights owners and produced by PWC on the costs of introducing a fair use exception, because it could provide no evidence of how it arrived at its conclusion. As noted in the summary of the Australian Productivity Commission report, "... these concerns are ill-founded and premised on flawed (and self-interested) assumptions". The Commission pointed out that "fair use does not equate with free use in any of the jurisdictions in which it operates, nor would it in Australia".

Fair use facilitates innovation and local creativity, current law does the opposite. As the US Supreme Court has repeatedly held, fair use "permits courts to avoid rigid application of the copyright statute when, on occasion, it would stifle the very creativity which that law is designed to foster". "Heavy handed policing and charging for every use will only create a disincentive for the creation of new works."

Why would fair use be good for New Zealand?
Fair use would open the purposes to which the current fair dealing exceptions can apply. This would provide a framework for considering new and innovative uses, without the need to go back to the legislative drawing board. It provides the breathing room for innovation and new uses, while ensuring that rights holders' legitimate interests are protected.

The development of massive storage capacity, powerful data manipulation techniques and graphics capability has transformed research and the acquisition of knowledge, and enabled data and text mining, the development of machine learning, and artificial intelligence.

Technologies such as these offer the opportunity to address some of the problems in the 21st century that threaten our very existence, such as climate change, food security, pandemics and drug resistant organisms. These technologies rely on machines to "read" millions of works. When machines read, they also copy. Requiring a licence for each one of these copies, which do not substitute for any work in the market and do not communicate the work to anyone, would shut down the technology. Companies such as Google explain that it is for this reason that they locate their most advanced engineering projects in fair use countries.

The Computer & Communications Industry Association, reporting on fair use and the US economy in 2017, noted that the fair use economy accounts for 16% of GDP and employs roughly one in eight Americans. It traced the roots of the importance of fair use to the *Sony* case.

We are a small country, far from the rest of the world, with a well-educated workforce. We are also renowned for our innovative solutions to problems. It makes sense to build on this by ensuring we have a copyright regime that fosters innovation, without affecting rights owners' economic rights.

We would do well to heed the words of Professor Peter Jaszi, testifying at the US House Hearings on fair use. Professor Jaszi wondered "why some of our most important foreign competitors, like the European Union, haven't figured out that fair use is, to a great extent, the 'secret sauce' of U.S. cultural competitiveness".

ARTIFICIAL INTELLIGENCE, LEGAL INFORMATION

Get ready for AI – practical steps for how to maximise the value of digital files


Richard Anstice

By Richard Anstice, member of ADLS' Technology & Law Committee

Today, many lawyers do not need artificial intelligence tools in their business. But, in the future, clients will require lawyers to use AI.

So, how does a reasonable practitioner get ready? Well, you get your data ready to be read and used by computers ... and fast.

AI promises a lot. In many cases it has not yet delivered. Lawyers are particularly cynical about it. We have spent our lifetimes relying on our own practical skills, working with paper-based documents.

But, the unfortunate fact is that AI software is getting pretty darned-good. The tools are smarter and more powerful. Some AI tools can already out-compete a lawyer. AI does things our clients increasingly want. A few applications are already a necessary part of legal practice.

It is clear that a law firm's files need to be ready for the future. If an urgent need arises (e.g. the prospect of litigation, or a substantial client due diligence), then the firm must be able to access good-quality digital data without delay.

AI tools need digital documents that the computer can read. For paper records, this means that a piece of technology called "OCR" is needed to read the text of documents and leave a digital record that a computer program can read.

So, every lawyer needs to start looking at the basic steps to prepare their client files for the future. What can you do?

1. **Plan the firm's investment in moving paper records to digital records**
Most firms need professional help with this. Make sure that OCR text-recognition is used. Also, in the digital system, each document needs to be properly recorded against client files. It can be costly. But it is an investment with future value.

2. **Consolidate records**
It is not OK to have some records on paper, some on a hard disk, some in email inbox, some in a document storage program, and some in a little crumpled heap on a shelf. It is time to consolidate those into a single digital location.

3. **Start storing every new document properly**
It all needs to go into a digital system – every file note, every contract, every email (out and in) every survey. Each document needs to get stored in a way that identifies the client and the matter. Documents can be date-stamped. Drafts can be tagged as draft. Invoice and admin records can be tagged.

4. **Destroy working copies when you are finished with them**
We all love bits of paper – use them, trash them, and rely on digital records for posterity.

5. **Have a plan for the "oldest inhabitant"**
There is no point spending money on new systems for staff to use, if a partner promptly ignores the new systems. Key documents are not available for the future if the partner has made sure they never entered the system. There needs to be a commitment to work together so that young and old alike use the firm's digital systems.

If client records can be searched, then every document in the practice can be a precedent for legal staff (i.e. without having to nag a partner to locate a precedent). If clients know a firm has great record-keeping, then the firm's records become a trusted asset for the client. If all the drafts and admin files are tagged, then less work is needed to hand a file to a client or another lawyer. Digital records that can be easily analysed give firms more options to take on new technology in future.

Fundamentally, good-quality digital records are an essential and valuable asset for the business. It is valuable intellectual property. Without that asset, a firm will be vulnerable to competition that uses AI effectively.

ARTIFICIAL INTELLIGENCE

The dangers of "do it yourself" AI

By Lloyd Gallagher, Director/Arbitrator/ Mediator, Gallagher & Co Consultants Ltd, and Convenor of ADLS' Technology & Law Committee

Today, the world of artificial intelligence - or AI - has taken centre stage in much of the world media, with headlines suggesting that AI has the ability to solve everyday computing problems now the norm in any given month.

Solutions for e-discovery, dispute resolution, automated contracts, and a host of other machine learning applications, are now available to the average consumer for a wide range of legal services, and have in turn given rise to articles and debates over legality, legal advice and responsibility.

But the ICT world has not been hampered by these debates. Recently, a number of internet start-ups have begun to provide boilerplate templates that allow the average user to "point and click" to an AI solution. New open source systems are touted as in-memory, distributed, fast, and scalable forms of machine learning that allow the individual to build models on big data, while providing an easy deployment in enterprise environments. It is suggested that it can apply to everyone – sports advanced analytics, fraud detection, claims management, and digital advertising solutions – to name but a few. But what is this kind of AI all about?

AI in this form is an analytical interface for Cloud computing, providing users with tools for data analysis. Its design is not standalone – it is predictive modelling based on analysis of data in the Cloud. Big datasets and Cloud data are simply too large to be analysed using traditional software, which is where AI assists – by providing data structures and methods suitable for big data. With AI, users are able to analyse and visualise whole sets of data without using the Procrustean strategy of studying only a small subset with a conventional statistical package. This opens up a range of possibilities – from finding the "smoking gun" in legal trials, to spotting patterns of behaviour in criminology.

In decision-making, the use of AI's statistical algorithms (which may include K-means clustering, generalised linear models, distributed random forests, gradient boosting machines, naive bayes, principal component analysis, and generalised low rank models) can provide a faster and more reliable way of retrieving data sets from large amounts of information which can then be culled to a predefined series for further analysis. Once that is complete, responses can be created – among other things, to assist with disputes, detect fraud, predict medication dosing, improve IVF outcomes, let you know when you are running out of milk (and where the best price to get it close to your house

Lloyd Gallagher

is) – in a user-friendly way.

But new AI boilerplates take matters one step further by providing an easy way to access complex data analysis tools in mere minutes. Such templates have been designed to assist in iterative real-time problem-solving. Iterative methods involve a mathematical procedure that uses an initial guess to generate a sequence of quick, approximate solutions for a class of problems. It works by dividing data into subsets which are then analysed simultaneously using the same method. The solutions that can be provided are only limited by the imagination of the developer, and solutions for e-discovery and large data sorting are just some of the first solutions developed in these kinds of designed templates.

However, designing such platforms has its pitfalls. The handling of boilerplate document completion and repetitive transactions raises legal issues (think the chatbot "DoNotPay" – "the world's first robot lawyer" – that ran counter to many of the legal protections provided to consumers). While this was not a flaw of the AI itself, it represents a flaw in the developers' thinking when it comes to the legal issues faced in advertising and developing their idea. Other issues such as privacy, protection of data, disaster recovery, hacker intrusion, and so on, all play a part in the success or failure of these boilerplate ideas. A lack of legal review will see clients facing stiff penalties under algorithms that are not properly designed and which may cause data loss.

Further, where AI template systems have been used to do things like determine discoverable documents, they will need to stand up to proper analysis. If flaws in data reporting become evident, this may lead to questions over whether the algorithm missed something – whether the approach taken was valid, and if the code in fact analysed the data or simply undertook pattern recognition?

By their very nature, boilerplate templates are rough drafts of code that parties can grab and drop into their coding design. This in itself can cause problems if they are adopted in raw form by clients with no change, or with a lack of knowledge as to how to properly apply a template to the required information set.

Data protection issues can also arise – for example, if boilerplate templates have been "cut and pasted" in such a way as to allow exploitation of flaws in the code by hackers. Any legal consequences of this would fall on the person using the code, not the original developer. This in turn raises further questions, such as who bears responsibility for any resulting data loss? Who becomes liable for an application that breaches the GDPR privacy principles? Is it the site provider? Should the provider have taken reasonable care in providing the code? Or is it the provider of the service that uses that code? While the hacker holds responsibility for misuse, the civil implications are likely to grow.

It is likely that a new range of litigation issues will crop up with the launch of sites like Build a Bot, Floatbot, Get Jenny, and so on, that will see the law of tort become more prevalent in IT legal disputes.

The message here is to take care when considering boilerplate template "point and click" solutions for quick and cheap answers to big data and e-discovery. Seek out the reliable sources and providers to handle your requirements, as any data loss will have far-reaching and very real consequences.

Further reading:

https://www.h2o.ai/customer-stories/

https://www.theverge.com/2017/9/11/16290730/equifax-chatbots-ai-joshua-browder-security-breach

https://www.technologyreview.com/s/609418/this-chatbot-will-help-you-sue-anyone/

https://techcrunch.com/2017/09/13/no-a-chatbot-cant-automatically-sue-equifax-for-25000/

https://www.stuff.co.nz/technology/102416329/nz-law-firm-developing-ai-that-will-improve-services-for-clients

https://botsociety.io/blog/2018/05/build-a-bot/

https://floatbot.ai/

https://www.smartdatacollective.com/will-hackers-eventually-use-big-data-ai-us/

http://www.experian.com/assets/data-breach/white-papers/2018-experian-data-breach-industry-forecast.pdf

https://www.information-age.com/data-breaches-financial-impact-123470254/

LEGAL INFORMATION, ACCESS TO JUSTICE

Democratising New Zealand's legal data

By Andrew Easterbrook, Rob Harte Lawyer

This article is about access to justice, and the difference between availability and accessibility of legal information.

Canadian scholar Roderick Macdonald suggested there are five parts (or "waves") of access to justice. One of those is the demystification of law, including access to legal information. In "Access to Justice in Canada Today: Scope, Scale and Ambitions", he said: "Improving access to legal education, to the judiciary, to the public service and the police, to Parliament and to various law societies is now seen as the best way of changing the system to overcome the disempowerment, disrespect and disengagement felt by many citizens."

Here in New Zealand, the Hon Justice Helen Winkelmann (in her 2014 Ethel Benjamin address) said: "In order to protect their rights, citizens must have a means of accessing and understanding substantive law." I agree: citizens should have tools available to them that assist with their understanding of legal information. This is more than basic availability of the information itself. It is about the accessibility of information.

Lawyers have good access to legal information by paying a lot of money to go to law school, and then paying expensive research subscriptions. Professional research sites give us information presented in a convenient, useful way, with high-powered search tools and the ability to navigate through clusters of related information. But the layperson misses out on that. For the most part, those tools are cost-prohibitive for non-lawyers. They must rely on what's freely available online.

Limited accessibility also poses difficulties for self-represented litigants in court. Their lack of legal knowledge was the most commonly reported problem in the Ministry of Justice's 2009 report,

Andrew Easterbrook

"Self-Represented Litigants: An Exploratory Study of Litigants in Person in the New Zealand Criminal Summary and Family Jurisdictions". In the same study, self-represented litigants said it was difficult for them to obtain information about legislation and case law on the internet.

Fortunately, the New Zealand government has an excellent policy on making data open – in the second National Action Plan, it commits to improving open data access and principles, and tracking the progress and outcomes of open government data release.

In the legal research area, NZLII has done an outstanding job of making a huge amount of case law available freely online – and has done so with limited resources. The amount of case law available online exceeds 100,000 judgments. However, these files are in an archaic format – PDF – which eschews the structure and interoperability necessary for text analysis, for print fidelity, and portability. This means that, before an open legal data platform can be made, the files must first be processed and the valuable information extracted.

In 2016, I was thinking about making such a platform. I reached out to an old friend of mine in the tech space with an idea transform New Zealand legal data from individual files into a rich, relational dataset, accessible to all Kiwis. We recently made that work public, and it's called "OpenLaw NZ" (https://www.openlaw.nz). By virtue of being open-source, anyone in the world may copy the code and adapt it for their own country's legal data. Any citizen can use OpenLaw NZ to use, manipulate and analyse that data in any way they think would be useful or creative, and make use of legal information in ways that suit their own needs, rather than just the needs of those who have spent four years at law school.

Citizens have the knowledge and capability to build platforms, and are being encouraged all over the world to embrace coding – from President Obama, to eight year-olds at school. Providing these people with easy access to high quality data unleashes its potential.

OpenLaw NZ is just one manifestation of the opportunity made possible through progressive government data policies. There is a plethora of government and legal data available online, and lots of exciting developments in the area. For example, the Service Innovation Lab at the Department of Internal Affairs is spearheading a lot of open government projects, and data.govt.nz has now published almost 6,000 datasets that touch upon almost all aspects of society.

Open data platforms promote the core tenets of a healthy democracy. It is not enough to make data available – the information must be accessible and consumable by both machine and person alike, using open standards. And, with the rise of cheap Cloud computing and an abundance of skilled technologists, there are opportunities to democratise data like never before.

BOOK

New Zealand Media and Entertainment Law

Authors: Rosemary Tobin and David Harvey

Contributing Author: Paul Sumpter

Media and entertainment law is a growing and rapidly changing area of law, governed by domestic legislation, and challenged by emerging new media such as online news and publishing, blogs, Twitter, Reddit, and Facebook.

New Zealand Media and Entertainment Law provides a detailed analysis in a modern framework. The authors weave the intricacies of new media through established case law, legislation and principles, while guiding legal and media professionals as they navigate the changing media landscape.

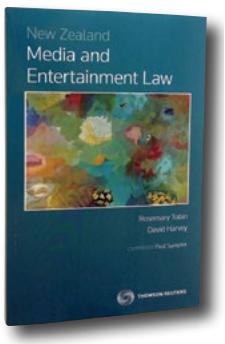
In addition to comprehensive analysis of traditional media law, this treatise explores harmful digital communications, the impact of online publication on defamation, regulation of classic and modern media authorities, and contempt in light of the "Contempt of Court" report released by the Law Commission in June 2017.

This book is an essential research and reference tool written for practitioners and students of media law, media and advertising agencies, as well as other professionals who must stay ahead of media regulation.

Price: $205.00 (plus GST)*

Price for ADLS Members: $184.50 (plus 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.

PRIVACY LAW

Privacy law for the Internet age

By James Ting-Edwards, InternetNZ

James Ting-Edwards

New Zealand's 25 year-old *Privacy Act 1993* governs the collection and use of personal information by all agencies.

Since 1993, the ways we collect, share and use information have changed radically. The use of computers, email and the Internet has moved from a niche specialist interest, to a core part of how most of us work. Computers have shifted from desk-bound furniture, to pocket-sized smartphones, which know our voices, faces and location.

Those are momentous changes in the treatment of our personal information. Despite limited legislative reforms, the *Privacy Act* has accommodated these changes remarkably well. At its core are information privacy principles, supporting harm-based responses by the Privacy Commissioner. This framework has enabled contextual responses to privacy breaches through physical documents being misplaced, through posts on social media, and through emails sent to the wrong address (one of the more common types of privacy breach).

Though its framework has accommodated change, our current *Privacy Act* is long overdue for an update. That update is now in sight, with a Privacy Bill currently before the Justice Select Committee. The Bill has its origins in the Law Commission's 2011 review of the Act, which in turn adopted analysis and recommendations from the "Necessary and Desirable" report of the Privacy Commissioner in 1998. The Bill itself was originally drafted five years ago. That history reveals a series of delays to a very important legal framework.

Our privacy law is of vital importance in the Internet era. As recognised in Article 12 of the Universal Declaration of Human Rights, privacy is a basic right. Privacy law is also among the broadest legal frameworks affecting New Zealanders, because it governs the use of our information by all agencies: government departments, businesses, and not-for-profits. Privacy law is central to the potential and risks of new technologies. To get the benefits of machine learning and other technologies, we need to know our information can be shared and managed in a way that respects our privacy. As drafted, the Bill retains the core features of the current framework. Still at its heart are the information privacy principles, and harm-based responses by the Privacy Commissioner to breaches of privacy. Proposed new privacy protections include mandatory breach reporting, conducting due diligence vetting before sharing data overseas (for example to a Cloud provider), and a new power for the Commissioner to issue compliance notices requiring an agency to take steps in relation to privacy issues.

Submissions on the Bill reflect the importance of updating our privacy law, and getting it right. The 165 submitters include privacy advocates, legal experts, businesses and individuals. Across the board, submissions express strong support for updating and improving our privacy protections. Lines company Vector, which recently suffered a large breach of customer data, joins Xero, TradeMe and Bell Gully, in supporting mandatory reporting of data breaches. The question raised by submitters is not "should we have breach reporting?", but "what should be the reporting threshold?" There are calls for the reporting threshold to be raised, and couched in objective terms on a "reasonable person" standard, to better align with reporting thresholds in Australia, and under the European Union's General Data Protection Regulation. I should note that the InternetNZ submission, which I was involved in writing, is among those calling for this change to the Bill.

The most important question remaining is whether the current Bill can get our law up-to-speed for the technologies we use now, and those we will be using over the next decade. With a Bill drafted five years ago, in an area that so affects all New Zealand businesses, and all of us as people, it is important that new proposals can be adequately tested through consultation.

TECH FOR LAWYERS

Review of Wayback Machine internet archive

Reviewed by Arran Hunt, Principal, Virt Law

The Wayback Machine (WBM) is one of those interesting websites that you don't think you'll ever need, but enjoy looking at anyway just for the nostalgia.

Then, your client has an unusual requirement, and its archive is a solution.

The WBM archives websites as they appear, keeping a record of that website's look and wording as at a particular date. More visited websites are likely to have more dates for which the page has been saved, but most websites should have something historical.

For example, adls.org.nz has been archived 595 times since 20 December 1996 (screenshot below of the first archived page):

Archived pages are not always evenly spread – there may be several on one day, and then nothing for a few weeks. However, unless the base website changes daily, this should be sufficient to at least see the static text and overall website design.

Some websites (notably newspaper websites) do not allow the archiving of their website. The same option is available to any website, so it is possible that others have also decided to bow out.

However, many websites would either not be aware of the WBM, or see no issue with being included.

The same method to avoid being included in the WBM can also impact how search engines (such as Google) rank a page, so there is a level of encouragement for websites to be included.

When this does come in useful is when your client has an historical dispute, and information provided on a party's website at the time is of use. For a recent matter regarding bank security, I was able to see what the bank's website had stated about its security, something which may not have been available directly from the bank.

Whether for a humourous look at the past, or as a tool, the WBM is a handy website of which all lawyers should be aware.

https://archive.org/web/

ADLS COMMITTEES

Committee membership applications 2018-2020

ADLS has a proud history of contributing to the law and the legal profession through its members and their participation in its Committees.

Seventeen ADLS Committees operate at present, comprised of volunteers who carry out a wide range of activities in their specialist areas. Committee members draft submissions, meet with government departments and the courts, contribute to Continuing Professional Development (CPD) programmes and partake in collegiality events.

Committee appointments will be for a two-year term aligned with the ADLS financial year, from October 2018 to September 2020. Successful Committee applicants appointed by ADLS Council will be notified in mid-late September, with the first Committee meetings taking place in October.

Applications for membership on the below-listed Committees for the 2018/2020 term are now open.

ADLS encourages applications from members throughout New Zealand – attendance at meetings can be accomplished not only by physically attending the meetings, but also by remote participation via phone and video conferencing.

Aspiring Committee members, as well as existing Committee members wishing to remain on their current Committee(s), should apply online at https://www.adls.org.nz/for-the-profession/2018-20-committee-application/ by **5pm, Monday 3 September 2018**.

*Please note that Committee appointments cannot be confirmed unless the applicant is a member of ADLS. Membership must be maintained during the course of the Committee appointment.

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

- Civil Litigation
- Continuing Professional Development
- Courthouse Liaison
- Criminal Law
- Documents & Precedents
- Employment Law
- Environment & Resource Management Law
- Family Law
- Health and Safety Law
- Immigration & Refugee Law
- Members' Special Fund
- Mental Health & Disability Law
- Newly Suited (for those new to the profession, from graduation to five years' PQE)
- Property Disputes
- Property Law
- Technology & Law
- Trust Law

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

TECH FOR LAWYERS

Review of Winmerge – PDF comparison

Reviewed by Arran Hunt, Principal, Virt Law

Winmerge does the simple job of comparing two documents or folders and telling you where the differences are.

That might sound like an unusual requirement, but its value stands out when there is a suspicion that a former employee, on leaving, deleted random files or folders from the company files. After running Winmerge, IT support staff should be able to retrieve the now identified missing files.

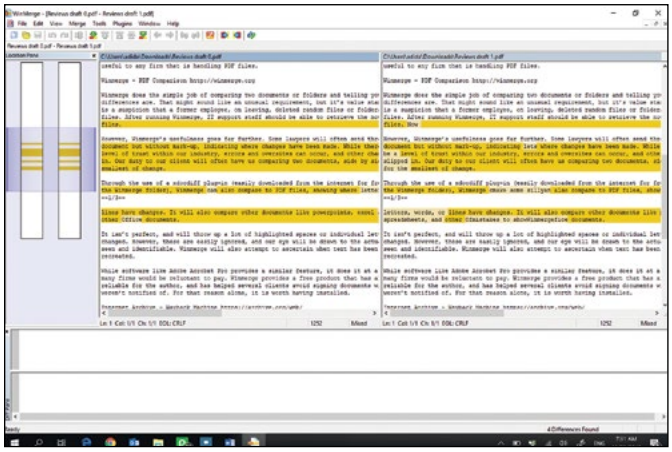
However, Winmerge's usefulness goes far further. Some lawyers will often send through an updated document but without mark-up, indicating where changes have been made.

While there should be a level of trust within our industry, errors and oversights can occur, and other changes can be slipped in. Our duty to our client will often have us comparing two documents, side by side, looking for the smallest of change.

Through the use of an xdocdiff plug-in (easily downloaded from the internet for free, and saved within the Winmerge folder), Winmerge can compare two PDF files, showing where letters, words, or lines have changed. It can also compare other documents like PowerPoints, Excel spreadsheets, and other Office documents.

Installation isn't as complicated as it would seem:

- download and install Winmerge;
- download the xdocdiff file, extracting the contents to the Winmerge folder;
- load Winmerge, go to plugins, click enable and auto unpack;
- Winmerge is then ready to use;
- click File>Open, and select the files you want to compare.



It isn't perfect, and will throw up some highlighted spaces or individual letters which haven't changed. However, these are easily ignored, and our eye will be drawn to the actual changes, easily seen and identifiable. Winmerge will also attempt to ascertain when text has been moved but not recreated.

While software like Adobe Acrobat Pro provides a similar feature, it does it at a substantial cost that many firms would be reluctant to pay. Winmerge provides a free product that has always proved reliable for the author, and has helped several clients avoid signing documents with new clauses we weren't notified of.

For that reason alone, it is worth having installed.

http://winmerge.org

Featured CPD

Privacy Breaches: Best Practice Advice for the Present (and the Future) – FINAL NOTICE

This seminar will consider the implications of breaches under the Privacy Act 1993 in its present form as well as addressing possible changes likely to occur including mandatory reporting and possible exceptions.

Learning Outcomes:

- Learn more about voluntary breach notification under the Privacy Act as it presently stands, why you should notify the Office of the Privacy Commissioner, actions to take, as well as the intersection between privacy compliance, governance and risk management and oversight.
- Understand better the requirements of overseas data breach notification regimes, and the steps that need to be taken to comply with the regimes including the consequences of not notifying the relevant bodies.
- Gain insights into what the future under an amended Privacy Act in New Zealand might be like including mandatory breach notification, steps to compliance and what will happen if you or your client fails to notify.

Who should attend?

Lawyers and practice managers who are responsible for privacy matters and those with clients who may require advice from time to time on this topic.

Seminar Livestream
CPD 2 hrs
Tue, 28 Aug
4pm – 6.15pm
Presenters
Michael Wigley, Principal, Wigley and Company
Katrine Evans, Senior Associate, Hayman Lawyers
Chair
Katherine Gibson, Director, Gibsons Law

The End of a Franchise – Considerations and Consequences – FINAL NOTICE

This seminar will introduce the ways in which a franchise can come to an end; discuss options and consequences for a franchisee or franchisor where franchisee breach or performance could lead to termination; set out franchisee options for early exit; cover wrongful termination; and look at post-termination considerations such as restraint of trade and ownership of goodwill in the business.

Learning Outcomes:

- Become better informed about what the provisions relating to term and termination really mean, when advising potential franchisees in their due diligence prior to signing a Franchise Agreement.
- Gain insights into potential legal issues and options when advising franchisors or franchisees where the franchisee is in default and their franchise could be terminated, or the franchisee wishes to exit without cause before the term has ended.
- Receive an update on case law and trends in enforcement of restraint of trade and the penalties doctrine as they apply to franchising.

Who should attend?

Commercial lawyers, litigators and general practitioners who act, or may be approached to act, for a franchisor or franchisee (at the outset or subsequently).

Seminar Livestream
CPD 2 hrs
Thu, 30 Aug
4pm – 6.15pm
Presenters
Sarah Pilcher, Principal, The Franchise Lawyer
Deirdre Watson, Barrister

Providing Initial Legal Advice

You get a call in the middle of the night from the police station, what should you do? Should you attend in person? Should you advise the client to make a statement? This is your opportunity to provide critical advice at a crucial time.

Learning Outcomes:

- Gain an understanding of the different types of offences that you will likely encounter such as EBA, traffic offences, bail and domestic violence issues.
- Learn more about administrative requirements you have under the Police Detention Legal Assistance.
- Gain practical insights into how you can respond to a cold call from the police station and the type of initial advice you could give.

Who should attend?

All lawyers practising in criminal law including Youth Advocates, especially juniors or those seeking a refresher.

Webinar
CPD 1 hr
Wed, 5 Sep
1pm – 2pm
Presenters
Mark Edgar, Barrister
Peter Tomlinson, Barrister

Immigration, Refugee and Protection – Appeals and Judicial Review: To the High Court and Beyond

High Court appeals and judicial reviews whether against IPT decisions or other decisions made under the Immigration Act 2009 or direct to the High Court can be complex and present practitioners with a plethora of potential procedural and substantive issues. By providing a procedural road map, an understanding of the legislative scheme and its interpretation by the courts, advice on important factors to consider when evaluating the merits of a case, and tips on the drafting of the frequently encountered documents, this seminar is designed to give lawyers the confidence to take immigration, refugee and protection matters to the High Court and beyond.

Learning Outcomes:

- Understand better those situations where an immigration, refugee or protection matter is appropriately advanced to the High Court and the statutory requirements to be satisfied – including time limits and the situations when it is necessary to first obtain leave.
- Receive guidance on typical procedural steps and documents involved in an appeal or application for judicial review concerning an immigration, refugee or protection decision in the High Court and on appeal above that court.
- Learn more about matters that commonly arise in the immigration, refugee and protection areas including legal aid eligibility, court fees waiver, confidentiality obligations, credibility issues, interim relief, dealing with counsel error, and the application of the New Zealand Bill of Rights Act 1990.

Who should attend?

All practitioners practising in the areas of immigration, refugee and protection law. The seminar may also be of interest to litigators who might be involved in this area of law in the future as well as immigration consultants.

Seminar Livestream
CPD 1.5 hrs
Thu, 6 Sep
4pm – 5.30pm
Presenter
Ian Carter, Barrister
Chair
The Honourable Justice Palmer

CPD in Brief

Essential Risk Management: Using Indemnity Clauses to Best Advantage

The balancing of risk is an essential aspect of commercial transactions. In many instances, indemnity clauses provide a very useful facility to secure the position of parties. However, it is worth considering whether such clauses are really necessary in a contract and, if they are, how they might be used to best advantage to clarify the client's expectations and to avoid conflict if possible.

Presenters: **David Broadmore**, Partner, Buddle Findlay; **Aaron Sherriff**, Partner, Duncan Cotterill

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

Seminar Livestream
CPD 1.5 hrs
Tue, 11 Sep
4pm – 5.30pm

GST for Property Lawyers Workshop (Auckland)

GST and the Compulsory Zero Rating (CZR) regime remain a constant headache for property lawyers; even experienced ones. This practical workshop, working in small groups, will focus on practical examples and scenarios, and will provide guidance to practitioners on the vexing issues of GST and CZR and how to deal with problematic situations. Limited places available, register now to avoid disappointment.

Presenters: **Allan Bullot**, National Leader – Indirect Tax, Deloitte; **Jeanne du Buisson**, Director – Tax, Deloitte; **Joanna Pidgeon**, Partner, Pidgeon Law

Workshop
CPD 2 hrs
Thu, 13 Sep
4pm – 6.15pm

The Replacement PPSR: What Lawyers Need to Know and Do Pre & Post 1 October

Three years in the making, the replacement PPSR and website go live on 1 October. If you are a legal professional who deals with the PPSR occasionally or often, whether for searching and/or registration, then there are steps you need to take to be ready. This webinar, taking place during the early onboarding period, will cover the key changes to the PPSR and Regulations; actions required both before and after 1 October; and key functionalities for legal professionals.

Presenter: **Agnese Abelite**, Senior Stakeholder Engagement Advisor, New Zealand Companies Office, MBIE

Webinar
CPD 1 hr
Wed, 19 Sep
12pm – 1pm

Your Legal Business: Employing Staff

Providing a roadmap for the legal and recruitment aspects of employing staff, this seminar in the Your Legal Business series will cover the 'lifecycle' of the employment relationship and include content on employer obligations, employee demands and trends in the market.

Presenters: **Simon Lapthorne**, Executive Partner, Kiely Thompson Caisley; **Jarrod Moyle**, Managing Director, Legal Personnel (2017) Limited

Chair: **Sandra Gilliam**, People Director, Kensington Swan

Seminar Livestream
CPD 2 hrs
Thu, 20 Sep
4pm – 6.15pm

The AML/CFT Workshop (Auckland)

The AML/CFT regime is now a reality. The implementation of compliance programmes is likely to have been a steep learning curve for practitioners with numerous issues, both practical and interpretative, arising and answers to problems not always easy to find. With numbers strictly limited, this workshop will provide a great opportunity for lawyers and compliance officers to raise their problems and to discuss potential solutions with an AML/CFT expert. Registrants are encouraged to send through their questions prior to the workshop.

Presenter: **Fiona Hall**, Barrister and Solicitor

Workshop
CPD 2 hrs
Tue, 25 Sep
3pm – 5pm

CPD Pricing

Delivery Method	Member	Non-Member
Webinar (1 hour)	$75 + GST	$105 + GST
Seminar (in person)	$125 + GST	$180 + GST
Seminar (livestream)	$125 + GST	$180 + GST
On Demand (1-hour recording)	$85 + GST	$120 + GST
On Demand (2-hour recording)	$140 + GST	$200 + 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.

ADLS EVENT

East Auckland Lawyers' Lunch

ADLS invites practitioners to join us for the annual East Auckland Lawyers' Lunch on Tuesday 4 September 2018, at Fisher House in East Tamaki.

These lunches provide a great opportunity to meet and network with fellow practitioners in your area, and to discuss with ADLS how we can further support you in your professional career.

Date & time: Tuesday 4 September 2018, from 12.30pm

Venue: Fisher House, 117 Kerwyn Ave, Highbrook, East Tamaki, Auckland

Registration: $29.00 (incl. GST) for ADLS members;
$34.00 (incl. GST) for non-members.

*Register before **Tuesday 28 August 2018** to secure your spot, subject to availability. Visit 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.*

ADLS EVENT

Hamilton Cocktail Function

Following the success of our previous events, ADLS again invites Hamilton practitioners and practice managers to be our guests at a special cocktail function to be held on Thursday 6 September 2018, at The Verandah in Hamilton.

The evening will be hosted by ADLS President Joanna Pidgeon and CEO Sue Keppel. We'd like to have the opportunity to learn more from you about the ways in which ADLS may be able to continue to provide support to the legal profession in Hamilton.

We hope you are able to attend, and look forward to meeting with you and discussing further how we might be of assistance in the year ahead.

Date & time: Thursday 6 September 2018, 5.30pm

Venue: The Verandah, Hamilton Lake Domain, Rotoroa Drive, Hamilton

Registration: There is no cost to attend this event, however, RSVP is essential.

*Register before **Thursday 30 August 2018** to secure your spot, subject to availability. Visit adls.org.nz to register; alternatively, contact adls.events@adls.org.nz or phone (09) 303 5287. ADLS' standard cancellation policy applies for this event.*

ADLS EVENT

Rotorua Lawyers' Lunch

Following the success of our inaugural lunch in 2017, the second annual Rotorua Lawyers' Lunch is being held on Wednesday 12 September 2018, at Terrace Kitchen.

These lunches provide a great opportunity to meet and network with fellow practitioners in your area, and to discuss with ADLS how we can further support you in your professional career.

Date & time: Wednesday 12 September 2018, from 12.30pm

Venue: Terrace Kitchen, 1029 Tutanekai Street, Rotorua

Registration: $25.00 (incl. GST) for ADLS members;
$30.00 (incl. GST) per person for non-members.

*Register before **Wednesday 5 September 2018** to secure your spot, subject to availability. Visit 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 Rotorua Lawyers' Lunch is proudly sponsored by MAS.

ADLS EVENT

Christchurch "Meet the Judiciary and QCs" evening

ADLS invites newly suited lawyers in the Canterbury region to our annual "Meet the Judiciary and QCs" evening, being held on Wednesday 12 September 2018 at The George in Christchurch.

ADLS is committed to supporting lawyers as they embark upon their legal careers. We encourage your attendance at this event to further the relationship between junior and senior members of the profession.

Don't miss this valuable opportunity to meet with members of the judiciary and Queen's Counsel in a collegial setting, where you can speak with these senior members of the profession candidly and gain from their insight and experience.

Space at this event is limited, so register now to avoid missing out.

Time & date: Wednesday 12 September 2018, 5.30pm

Venue: The George, 50 Park Terrace, Christchurch

*Register before **Wednesday 5 August 2018** to secure your spot, subject to availability. Visit adls.org.nz to register; alternatively, contact adls.events@adls.org.nz or phone (09) 303 5287. ADLS' standard cancellation policy applies for this event.*

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.

Alexander Morrison CAWLEY, Late of The Booms Rest Home, Thames, and previously of 7B Lee Street, Whitianga, Aged 90 (Died 05'07'2018)

Anne Frances SHANLY, Late of Auckland, Aged 96 (Died 17'07'2018)

Averil Miriam ROBINSON (also known as Averil Miriam CHANDLER), Late of 33 Shelly Beach Road, Helensville, Aged 46 (Died 25'07'2018)

Denis Tenny VAADUSUAGA (also known as Tenny Taumata VAAFUSU), Late of 19 Sunningdale Street, Wattle Downs, Auckland, Aged 62 (Died 12'06'2018)

Brian Lawrence WASON, Late of 111 Old Railway Road, Kumeu, Auckland, Aged 77 (Died 23'04'2018)