LAW NEWS

Sep 10, 2021
Issue 31

Inside

TECHNOLOGY

Special feature: Technology and the law

P03-14

TECHNOLOGY

How lawyers are putting their firms at risk

P06

How ‘virtual assets’ impact on LAWYERS AND THEIR CLIENTS

ADLS

adls.org.nz

Contents

07
CYBERATTACK DELEGATION RULES
Slack security could bring down your firm

08
DIGITAL NATIVES ISOLATON INNOVATION
How technology is changing the teaching of law

14
ANTI-TRUST TECHNOLOGY CONTENT
A new look at tech and competition law

10-13


Photo: BrianAJackson / Contributor / Getty Images
When must you report a data breach?

15
EVENTS

16-17
FEATURED CPD

18
CPD IN BRIEF

LAW NEWS

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

Editor: Jenni McManus
Publisher: ADLS

Editorial and contributor enquiries to:
Jenni McManus
021 971 598
Jenni.Mcmanus@adls.org.nz
Advertising enquiries to:
Darrell Denney
021 936 858
Darrell.Denney@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.**

Cover:
George / Getty Images

CRYPTOCURRENCY/FINANCIAL SERVICES

Lawyers **urged to upskill** on 'vitual assets'

The fact that it's taxed like property means it will probably be slower to be adopted. No-one will go out and buy a coffee with bitcoin if it creates a taxable event every time

Diana Clement

Cryptocurrency is all the rage. But how – and should – it be regulated and is our law **fit for purpose?**

These are the questions Parliament will grapple with as it gets to grips with an inquiry into the current and future nature, impact and risk of cryptocurrencies. Submissions closed earlier this week.

The inquiry, by the Finance and Expenditure Committee, is considering the nature and benefits of cryptocurrencies, the risk they pose to the monetary system, financial stability and users, how they are used by criminal organisations and to establish whether they can be adequately regulated. These issues affect a wide range of lawyers from family to insolvency and everything in between. Even if they don't know it.

Other countries' regulators are also becoming worried. *The Economist* recently reported that 12 years after bitcoin was born, governments were still struggling with cryptocurrencies. Britain has banned Binance, a crypto exchange, and the EU's regulators want transactions to be more traceable. On 3 August Gary Gensler, the head of the US Securities and Exchange Commission, said cryptocurrency markets were "rife with fraud, scams and abuse" and called on Congress to give his agency new regulatory powers.

Governments, *The Economist* said, have an obligation to fight the deception, tax evasion and money laundering that plagues the crypto world. "Police seizures of bitcoin suggest they are becoming more zealous. The harder issue they must grapple with is whether cryptocurrencies threaten the financial system."

Australia is talking about enhancing its economy and environment for business while our politicians are still asking what a cryptocurrency is

Crypto is not just currencies. There is a growing market behind the scenes around virtual assets, says Binu Paul, specialist lead, FinTech at the Financial Markets Authority (FMA).

In fact, the word 'crypto' is something we should leave behind, according to Lloyd Kavanagh, financial services partner at MinterEllisonRuddWatts. "The better term is 'virtual assets'." These are fast becoming part of mainstream business, not something traded illicitly on the dark web, and are a legitimate asset class that has entered the mainstream, Kavanagh says. "It's really important that lawyers, journalists, politicians, government officials and businesspeople understand it."

The growth of virtual assets makes the subject relevant to lawyers in a wide variety of disciplines such as mergers and acquisitions, insolvency, family, estate planning, tax and the environment, says James Cochrane, a partner at Stace Hammond.

All lawyers should be considering the issues, adds Kavanagh. Too often there is a disconnect between those in the know who see the big picture and business opportunity, and the rest of New Zealand which hears the word 'cryptocurrency' and thinks of the dark web.

Terms of reference

Kavanagh says it's essential the select committee considers the bigger issues for the business world. "We are in a period of transformation and coming into a new age. Digital assets and mediums of exchange are having an increasingly important role, and we need to have the appropriate balance of regulation so New Zealand can participate," he says.

"I do have a few concerns with the [inquiry's] terms of reference. You could read them as having a somewhat negative frame." He accepts there are concerns about crime and the misuse of virtual assets but says cash can also be misused.

He contrasts the terms of reference in New Zealand's inquiry with those of the Senate Select Committee in Australia.

"Australia is talking about enhancing [its] economy and environment for business while our politicians are still asking what a cryptocurrency is.

"It's important that New Zealand develops additional lines of business activity that employ New Zealanders and we export their services, which can be carbon-light compared to, or in addition to, our traditional activities.

"That's one of the really useful things about having the select committee, provided that the terms of reference are wide and not seen as just a narrow compliance issue. It's actually about building New Zealand's economy to be a better place and exporting services rather than exporting our best people to do their work in Australia or Singapore or the US. Hopefully, despite the potentially negative terms of reference, it will take a broad positive view about the part virtual assets can play in the New Zealand economy."

Legitimate business

Increasingly, New Zealand business is taking an interest in virtual assets. For example, Greymouth-based Ruby Play Network is **raising equity** through online investment market Snowball Effect in an offer where investors will get a mixture of equity and decentralised RUBY token rights.

Continued on page 04

Continued from page 03

It's not the only start-up looking to launch virtual asset-related products here. The FMA's Paul chairs the FinTech group of the Council of Financial Regulators. Earlier this year members of the council, which includes the FMA, Inland Revenue Department, Commerce Commission, Treasury and MBIE met with the Department of Internal Affairs (DIA) and 26 start-ups, around 14 of which have businesses related to virtual assets, says Paul. All were seeking guidance from the regulators.

"So, there's a lot of activity where people are looking to experiment, looking to innovate in that space," Paul says. "It will take time for them to have a product that's in the market, but it's happening."

Legal advice

Virtual assets touch more areas of the law than just financial services and crime, Cochrane says. "As legal advisors, we are cognisant of the expanding pervasiveness of crypto assets, throughout the global financial and commercial landscape, and the impact this has [or will soon have] on legal advice."

Kavanagh points to the FMA-Retail-Investor-Platforms-Research, a survey which, amongst other things, found 28% of investors have some form of virtual asset holding and 34% intend to be investing by next year. "That will make it highly relevant that all lawyers, especially those working in trusts and estates, or relationship property, have some understanding of the topic."

Cochrane says virtual assets will increasingly impact on the work of relationship property lawyers. "What are the tax implications if you were to do a separation agreement? And, for estate planning lawyers, how does a person ensure their anonymous virtual assets pass down to their beneficiaries? Who holds the key to the wallet? Without it, the money is lost."

He says a growing number of New Zealanders hold virtual assets and any lawyer who needs to do client and anti-money laundering (AML) due diligence will increasingly need to consider virtual assets.

"Is that a scam, [or a] suspicious transaction? How do you deal with [potentially] tainted coins? If you're acting for the vendor in a transaction, you might want to insist that the transaction goes through a regulated exchange to avoid putting the client at risk of AML implications."

In mergers and acquisitions, for example, lawyers need to be mindful when conducting virtual asset-related due diligence to ensure clients are adequately protected and are not breaking the law.

It also touches insolvency. Cochrane cites the New Zealand High Court decision in *Ruscoe & Moore v Cryptopia Limited 2020 (in liquidation)* [2020] NZHC 728. The application concerned the competing interests between Christchurch-based exchange Cryptopia's account holders and creditors.

Being a novel case for New Zealand, Cryptopia's liquidator Grant Thornton New Zealand filed an application to the High Court, seeking directions (under s 248 of the Companies Act 1993) about the legal status of virtual assets in New Zealand.

The High Court determined that virtual assets are property, although not legal tender, which is in line with decisions in the United States and has implications for taxation, Cochrane says.

The case, adds Kavanagh, shows the 'wonderful flexibility' of common law and the New Zealand courts, which had to grapple with an entirely new environment.

In April this year, the owner of a Waiheke property became the **first home bought using Bitcoin**. Property lawyers will begin to see virtual asset transactions appear frequently. These examples show how virtual assets have come in from the cold and are now viewed by the mainstream as an asset class, Cochrane says.

Not legal tender

Few countries so far have declared virtual assets to be legal tender. This creates an issue with businesspeople who have made large sums of money in virtual assets and want to use that money to start business here and employ people.

Virtual assets have just become legal tender in El Salvador (alongside the US dollar) and other Latin American countries could follow suit.

Tonga is another, thanks to Mata'i'ulua 'i Fonuamotu, Lord Fusitu'a, a member of the royal family and Tonga's Parliament, who is a huge advocate of virtual assets. Tonga, like many countries, relies heavily on remittances from its diaspora, but a

Continued on page 05

If it's too complex. If it's too scary. If the law is not fit for purpose. Then we're potentially going to stifle innovation, and we are going to miss out on a huge opportunity for New Zealand to grow its productivity as a nation in the tech space

James Cochrane

Lloyd Kavanagh

Binu Paul

Continued from page 04

good chunk of those funds are lost to remittance companies. Lord Fusitu'a has been quoted as saying he believes that by embracing virtual currencies Tonga can become more competitive and wealthier. Spanish lawmakers are backing legal initiatives to legitimise the cryptocurrency for mortgage and insurance purposes.

What are the tax implications if you were to do a separation agreement? And, for estate planning lawyers, how does a person ensure their anonymous virtual assets pass down to their beneficiaries? Who holds the key to the wallet? Without it, the money is lost

Work in progress

Jurisdictions around the world are coming to terms with virtual assets and it's less wild west and more like a work in progress in 2021.

The market is not completely unregulated in New Zealand. Applicable laws include the Financial Markets Conduct Act 2013 (FMC Act), the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (AML/CFT Act), and the Financial Service Providers (Registration and Dispute Resolution) Act 2008.

For virtual assets and services to fall under the FMA's remit the providers must be domiciled in New Zealand, Paul says. If not, investors are not protected by New Zealand law, even if they are taxed here.

New Zealand has only four categories of financial products: equities, bonds, managed investment schemes such as funds and derivatives, which need a licence from the FMA. If a virtual asset had the form and function which made it resemble one of these four categories, it would need to be licensed, says Paul. Each product is considered individually.

Even if the product can't be regulated, a New Zealand company providing a financial service needs to be registered on the Financial Service Providers Register (FSPR), says Paul. Consequently, the provider needs to belong to a dispute resolution service such as the Insurance & Financial Services Ombudsman or Financial Services Complaints Limited.

Some areas of the law need to be modernised, Kavanagh says. One example is the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (AML/CFT Act), which many lawyers grapple with.

The OECD's Financial Action Task Force (FATF) noted in its recent review that New Zealand's regime needs work. Relevant parts of the legislation were drafted in 2009. The DIA has issued various forms of guidance, but they don't connect well to the legislation, says Kavanagh.

Tax implications

The decentralised nature of virtual assets poses an issue for tax authorities.

The IRD has no special tax rules for virtual assets. It does, however, provide **guidance to taxpayers** thanks in part to *Ruscoe & Moore v Cryptopia* where the court ruled that virtual assets are property. That allowed the IRD to treat virtual assets accordingly. Tax is applied when the currency is bought or sold, rather than on unrealised gains. It's not necessary to cash it out for a tax obligation to exist. That makes it similar to property.

The fact that it's taxed like property means it will probably be slower to be adopted, Cochrane says. No-one will go out and buy a coffee with bitcoin if it creates a taxable event every time. "There's a lot of complexity when you come to thinking about your tax."

Balancing act

The select committee considering cryptocurrencies will need to tread careful. Too much regulation could stifle innovation, meaning New Zealand could miss out on a huge opportunity, say both Cochrane and Kavanagh.

"If it's too complex. If it's too scary. If the law is not fit for purpose. Then we're potentially going to stifle innovation, and we are going to miss out on a huge opportunity for New Zealand to grow its productivity as a nation in the tech space," says Cochrane. "If you overregulate, then another nation will just pick it up. It's like Whack a Mole. If you ban all the mining in China, it just moves.

"I would like to see a balanced approach. I would like to see that they are not just looking within New Zealand," he says.

"My concern would be that we have legislation that is viewed as an opportunity to tax. And that stifles innovation in this sector."

The final word goes to Kavanagh who wants to point out that although bitcoin is energy-hungry, other newer assets such as ether (which uses the ethereum technology) are more efficient. ■

As legal advisors, we are cognisant of the expanding pervasiveness of crypto assets, throughout the global financial and commercial landscape, and the impact this has, or will soon have, on legal advice

How lawyers put their firms at risk

Users might not realise that if they use their firm password elsewhere, like on LinkedIn or Zoom, and if that system is hacked, the firm's systems are exposed

Andrew Easterbrook

This article is meant to scare some IT safety into you. The security of any system is only as good as the weakest link. Understanding how enables you to identify vulnerabilities that might be exploited.

In this article I explain how a typical law firm network and system might be set up and how its component parts create risk.

A common setup might be something like this: Employees normally work from a computer physically located in an office. Logins are required to access the computer and the computer automatically locks if there is no activity for about five minutes.

Once logged in, a user can access information on a server where client data is stored. That server might be located elsewhere in the office, a data centre, or an offshore cloud system accessed through a web browser. Access to client and firm data is managed by the firm's client management system (CMS). Storing any data outside that CMS is prohibited. Remote access is normally possible through a VPN or a web browser (like ActionStep).

Links in the chain

A system such as this relies on hundreds of linked components. A breach in any one of them could enable unauthorised access to your system. The most significant components are:

Devices

- **Office computers linked to the network.** An unauthorised person who can access an unlocked computer can do anything an authorised person can do.
- **Other computers on the same network.** This includes computers used outside the office (like those at home, connected through a VPN), devices in meeting rooms and devices connected to the wifi network. A device connected to a firm network might be able to:
  a) Access information stored elsewhere on the network and copy it;
  b) Infect other devices on the same network with malware or ransomware; and
  c) Compromise IT provider computers. The network security of your IT provider's systems could be a weak point. If your IT provider has full access to your system, any unauthorised access to their systems could expose your system in turn.

Andrew Easterbrook

Software

- **The firm's client management system.** That software, like most, is not likely to be developed entirely in-house. It will include pieces of code from public libraries which may have vulnerabilities that could put client data at risk.
- **Other software on computers with network access.** A computer runs programs. These tend to have access to everything the computer itself has access to. If a user installs a program on his or her computer, that program could do something unintended or malicious, causing loss. There is no good way to know exactly what any given application might do behind the scenes. So, there is no safe way to let users install programs of their choice.

People

- Users can't be trusted. Not necessarily because they are deliberate risk-takers but because often they don't understand that what they are doing is risky. For example, employees will try to get around security restrictions out of a genuine desire to make their job easier or simpler.
- Password security is very poor and the adoption of password managers is low. Users might not realise that if they use their firm password elsewhere, like on LinkedIn or Zoom, and if that system is hacked, the firm's systems are exposed. No online service is safe from potential data breaches: Yahoo, LinkedIn, Facebook, MySpace and Adobe have all suffered from significant hacks.

Some scenarios

Here are some examples to show how a vulnerability in one part of the chain puts all other parts at risk.

You allow remote access via VPN. If a staff member's home (personal) computer is infected with malware, that malware could jump across to your firm's network. If an employee's home PC is used by a teenager who downloads a pirated movie which turns out to be ransomware, and your employee then logs into the firm's network from that same computer, your firm network could be infected.

If an IT staff member working from home leaves his or her computer logged in, a flatmate or family member could easily gain full access to the firm's systems.

An inadvertent mistake made by an external software developer (eg, Zoom) might result in stored passwords not being encrypted. The software is then hacked and logins published. Logins are easily tied to the firm because they include the employees' email addresses. Your firm network can then be accessed and client data could be lost or misused.

What to do

There is no perfect solution. All computer systems are likely unsafe to some degree. You can mitigate some of the risks by (at a minimum):

- insisting all employees use password managers, randomly generated passwords and do not re-use firm (or any) credentials anywhere else;
- tightly controlling remote access and ensuring remote users are trained in security;.
- tightly controlling physical access to computers with network access; and
- separating networks so client data is not on the same network as client wifi. Only trusted devices should be allowed onto a network that can access client data.

Andrew Easterbrook is an associate at WRMK Lawyers. He is also a member of the ADLS Technology & Law Committee

SPECIAL FEATURE: TECHNOLOGY & THE LAW

Slack cybersecurity could bring down your law firm

Law firms are a honey pot, a place that individuals and companies will often keep their most confidential information

Arran Hunt

We'll get right to the point. Many partners are running their firms, or allowing them to be run, in a way that is detrimental to their clients. If the worst were to happen, and it is an ever-increasing hazard, partners could expect to lose any value they had in their firm as clients bail out in droves.

Cybersecurity and the risk of cyberattack still garners surprisingly little attention within the legal profession. Many firms who realise a lawyer needs to be involved seem merely to pass the issue of IT security to a junior staffer and consider it handled.

On 1 July 2021 we saw changes to the Lawyers and Conveyancers Act (Lawyers: Conduct and Client Care) Rules 2008 (RCCC). The most reported and discussed changes were those brought about by the Independent Working Group chaired by Dame Silvia Cartwright. However, other changes were also introduced. For this discussion, r10.11 expanded the old r10.4 as to the reasonable steps that needed to be taken to, in the updated wording, "ensure the security of and access to electronic systems and passwords, the protection of digital certificates and associated passwords, and the security of passwords, usernames, and personal identification numbers relating to electronic banking".

Amongst all the rules, this is the one that few lawyers would actively turn their minds to. Security seems to be something partners are willing to delegate to a third-party managed service provider (MSP). However, we would argue that such delegation is insufficient to satisfy the rules and such an approach could be detrimental to clients.

Delegation

Experts are valuable but responsibility under the rules cannot be delegated. Rule 10.11 requires the lawyer to take reasonable steps not merely to engage someone to handle security but also to ensure the job is done. Delegating a task does not meet those requirements.

The only truly secure system is one that is not used. Improper use by staff can negate any security put in place by the MSP. This could be as simple as leaving a password on a note by a PC, not having a phone properly secured or having an enabled network port in a meeting room.

MSPs are not lawyers, so are unlikely to understand all the obligations that might be required of you, whether under legislation, by the court or by clients. Firms should also not expect that of them.

Some MSPs may provide a service to a standard and in a manner that is dictated by their own preferences, or at the request of other clients. Such service levels may not be suitable to the needs of a law firm. For example, one MSP was storing a firm's files on a virtual server shared by another party. When that other party was hit by a cryptolocker, locking the files until a ransom was paid, the law firm's files were also locked as they were sharing the server. This led to the loss of a day of productivity for several dozen staff.

Treat security in a similar way to harassment or trust accounting

In another example, an MSP had a backup procedure that required manual retrieval of backups on a weekly basis. This meant files were backed up only weekly, creating a constant threat that the firm might lose a week's work had the server failed. To make matters worse, when during the 2020 lockdown no backups were taken offsite for almost two months. Any drive failure at that time would likely have ended the firm. The MSP did not make the firm aware of this failure until the country had gone to level 2.

These are just two examples of what can happen when a firm has followed the direction of an MSP or left security procedures completely in its control.

Arran Hunt

Neither situation is acceptable.

Other considerations

The preface to the rules also mentions the need to protect clients' privacy and confidentiality. This is partially covered by the correct application of r10.11. However, the Privacy Act 2020 should also be considered.

Part 6 of this Act, covered in more detail on pages 10-13, requires clients to be informed of any privacy breach that may cause serious harm. Because of the types of files firms hold for clients, almost any breach of privacy is likely to require that the client is notified. If a security breach occurs and it isn't clear if any files have been taken, you might need to notify all your clients that a breach has occurred. That would be significantly detrimental to a firm's continued operation.

Taking action

There seems to be a reluctance, especially from larger firms, to be actively involved in ensuring their systems and procedures meet these requirements. This needs to change drastically.

Law firms are a honey pot, a place that individuals and companies will often keep their most confidential information. They are the most tempting of targets, and bad actors are aware that firms are often run by people without the focus or aptitude for IT. Firms need to be more engaged in that security or risk an attack that will bring them down.

Treat security in a similar way to harassment or trust accounting. Each firm needs a security partner who can focus on ensuring r10.11 is followed. It is no less important than any other delegated role within a firm.

Arran Hunt is a partner at Stace Hammond and a member of the ADLS Technology & Law Committee

Please also see tech future, cybersecurity and comp law

The changing face of legal education

Ultimately, online learning can be isolating for everyone involved, which may impair the quality of teaching and learning

Amy Irvine & Andrew O'Malley Shand

Covid-19 has brought to the forefront the discrepancy between the digital skills we have and the skills we need. So, how are our universities responding?

In a recently-released strategic plan, University of Auckland vice-chancellor Dawn Freshwater said the university would prioritise education, research, insight and understanding across 'broad domains', including technology and digitisation. What does this mean for the University of Auckland's Law School? And how will this impact the legal profession?

Tertiary education has fundamentally changed in the past two decades. Bronwyn Davies, a teaching fellow at the university, makes the following points:

- the university teaches digital natives. Today's students are different from graduates of 20 years ago in how they learn and what they expect;
- the university must provide technology-based courses to recognise the growing confluence of technology and law; and
- the university must embrace AI and digital platforms as part of its teaching.

Ultimately, the goal is to provide education that better serves undergraduate students and improves academic understanding and employability, as well as professionals who want to return to university to upskill for the digital age.

The university's strategic plan aims to prepare students for a technologically-advanced future. This means improving students' practical digital skills and offering courses on areas shaped by technology, such as AI, cryptocurrency and data security.

Learning methods have changed dramatically in the past two years. It is now mandatory for lectures to be recorded and some courses are taught entirely online. Covid-19 has accelerated the digitisation trend.

New courses are being developed. One explores the intersection between law, technology and policy and others are likely to follow. Existing courses are being overhauled to reflect the importance of technological issues – for example, privacy law now has a greater focus on technology and this reflects students' increasing interest in pressing issues such as data protection rather than traditional privacy torts.

These changes are the tip of the iceberg. Students' uptake of technology-centric papers is encouraging and despite the occasional kink, technology provides massive advancements in both capacity and capabilities in teaching.

There is scope for the law school to engage with students and help them to prepare for the new wave of technologically-based legal issues.

But online learning has its drawbacks. It can be difficult for a lecturer, speaking to a screen, to gauge whether his or her students understand the content. Moreover, it can be difficult for a student to sit in front of a laptop for hours and feel he or she is getting an authentic university experience.

Big changes in how lawyers communicate with clients and colleagues, administrative innovations, implementation of AI and social media have radically transformed the way the profession operates and interacts

Ultimately, online learning can be isolating for everyone involved, which may impair the quality of teaching and learning. But technology has irreversibly changed the classroom experience and is not going away anytime soon. What matters is how the law school grapples with these issues to ensure the learning experience remains fulfilling for educators and students.

Amy Irvine

Andrew O'Malley Shand

Why should the legal profession care? It is evident that the profession is changing rapidly and fundamentally. Big changes in how lawyers communicate with clients and colleagues, administrative innovations, implementation of AI and social media have radically transformed the way the profession operates and interacts – not to mention the looming threat of automation.

Future graduates are uniquely placed to enter the legal profession and make meaningful contributions with in-demand expertise in these areas.

This requires the university to provide digital skills and courses and a culture to develop what researcher Matt Bartlett refers to as the 'innovation mindset'. This makes for better thinkers, graduates and lawyers.

Equally, professionals should have the opportunity to return to university to improve their proficiency in areas where law and technology intersect. Our educational institutions must reflect and support both students and professionals through this. Win-win.

Technology will radically change the legal profession. Education that fosters digital skills, knowledge of technology and legal issues and an innovative mindset is essential to confront these challenges.

Amy Irvine and Andrew O'Malley Shand are student members of the ADLS Technology & Law Committee

SPECIAL FEATURE: TECHNOLOGY & THE LAW

Why lawyers must be proactive in preventing cyberattacks

The easier targets are often small-to-medium-sized law firms that may lack the resources to prioritise cybersecurity or simply ignore it as an IT issue

Edwin Lim

As practitioners advising clients on data- and cyber-security as part of their technology transactions, we must practise what we preach. Ensuring we have appropriate measures in place to protect our systems and information from a cyberattack is paramount.

Covid-19 lockdowns have changed the way the world works and as remote working, even outside lockdown, becoming common, it has added to the mix of issues to consider from a cybersecurity perspective.

Cyberattacks, including viruses and infections, can wreak havoc on people and businesses. We need to ask how an attack might impact on our businesses and those of our clients and suppliers.

In 2016, the leak of 11.5 million confidential documents to a German newspaper through the alleged hack of global law firm Mossack Fonseca highlighted one of the main threats to law firms - hackers who target firms to steal client information and corporate intelligence.

Mossack Fonseca, established in 1977, didn't survive the economic and reputational damage and shut its doors in 2018. Earlier this year, top-tier Australian law firm Allens was caught up in a cyberattack after a third-party file-sharing system it used to share client information was compromised. The attack, on Californian cloud company Accellion, might have exposed highly sensitive information about one of Allens' biggest clients, Westpac.

While the threat of information theft is very much alive, ransomware attacks are now on the rise and causing significant disruption in businesses. We have only to go back a few months to see how a ransomware attack crippled the Waikato DHB.

Ransomware, a type of malicious software, denies its users access to their computer system or files, or threatens to publish information obtained from the compromised system unless they pay a ransom.

Edwin Lim

It is becoming common for law firms to be required to complete cybersecurity questionnaires at the request of their existing clients

Ransomware can get into a system through a phishing campaign - a type of email scam where unsuspecting users open an email attachment or link that contains the malicious software which is deployed in that system. The first sign of a ransomware attack is often a message that appears on users' screens, telling them they've been attacked and demanding a ransom, or if users are suddenly unable to access their computer or files.

These examples demonstrate why cybersecurity's importance is growing more critical as we witness new attacks on an unprecedented scale. This includes New Zealand law firms - large or small. The easier targets are often small-to-medium sized law firms that may lack the resources to prioritise cybersecurity or simply ignore it as an IT issue that doesn't affect them.

Cybersecurity is a business issue and it affects us all. It involves developing, implementing and maintaining robust staff training, policies, procedures and measures (technical, practical and organisational) to proactively protect all information and systems within your control.

Clients are becoming increasingly aware of the importance of cybersecurity and will want to know you've put all appropriate measures in place. It is becoming common for law firms to be required to complete cybersecurity questionnaires at the request of their existing clients, so clients understand how we protect their information. If they are given the opportunity to pitch for work from new clients, law firms are often required to describe what cybersecurity measures they put in place and the answers become part of the overall assessment.

It's no longer good enough to sit back and wait for a cyberattack to happen before doing anything about it. It's even worse if you think a cyberattack won't happen to you.

We have a positive duty as lawyers, whether in private practice or in-house, to prevent it from occurring in our businesses. As lawyers, our duty to protect data will almost always be over and above that of most other businesses.

Our duties as members of the profession and as fiduciaries to our clients extend to appropriate cybersecurity measures. Cybersecurity obligations also rest on company directors, as confirmed by the Institute of Directors, so as in-house or external legal counsel we should be ensuring company directors understand their obligations a

The consequences of a cyberattack to you and your business are boundless. The possibilities of financial, business and reputational damage are enormous and the possible routes of legal liability are continuing to increase. It's certainly no longer an excuse to say you didn't know what cybersecurity is.

Being proactive in mitigating the risks by keeping up-to-date with the latest threats and best practices is key. Be prepared, have your systems tested, train your staff, have a cyber response plan and take out cyber insurance. Think of these practices as a vaccination for your systems – they could prevent your systems from getting infected or greatly reduce the impact of an attack.

Edwin Lim is a partner at Hudson Gavin Martin, a commercial and corporate law firm specialising in technology, media and IP. Ed is also a member of the ADLS Technology & Law Committee

Navigating s113: how to handle a privacy breach

Breaches will capture the attention of partners and insurers, along with the media if the breach is notable

Lloyd Gallagher

Lloyd Gallagher

The Privacy Act 2020 requires agencies, firms and other organisations to report any privacy breach if serious harm, as outlined in s 113, is likely. But s 113 is subject to caveats designed to make the Act workable and leaves the decision to the Privacy Commissioner. The commissioner has provided some clarity on the meaning of serious harm but not the decision-making process. As s 118 creates an offence, it is important to understand what is expected.

Actions in response to a breach are likely to be scrutinised by the Privacy Commissioner and affected individuals and may be reviewed in litigation. In addition, a breach will likely capture the attention of partners and insurers, along with the media if the breach is notable, with consequences for reputation and further business. A breach may also bring unwanted attention under s 118 for criminal liability so any conclusion by an agency that it did not consider a breach to be notifiable will need to be justified as reasonable in the circumstances: s 118(3).

Agencies should consider retaining records about the breach and the assessment and mitigation actions taken. In Canada, for instance, cl 6 of the Breach of Security Safeguards Regulations requires that records be maintained for 24 months. The European Data Protection Board recommends that agencies document their processes and maintain an internal register of breaches, both notified and non-notified, including the process for determining what, where, how and why the breach was handled in such a way. Section 113 provides assistance with that process and we will discuss best practices here.

Reducing risk post-breach

Under s 113(a) the agency should first consider whether the actions taken since the breach occurred or was discovered have reduced the risk to below the s 113 threshold (risk of serious harm).

Examples of post-breach actions to reduce risk may include:

- Immediately containing the breach – for example, stopping the unauthorised practice, recovering the records, shutting down the system affected, revoking or changing computer access codes or correcting weaknesses in physical or electronic security.
- Initiating an investigation that may lead to a better understanding of the cause and limits of the breach. Preserve evidence for further assessments and develop a prevention plan.
- Ensuring those who need to know about the incident internally, and potentially externally, are made aware. Escalate internally as appropriate and inform anyone responsible for compliance.
- Creating alerts and warning partner agencies of the issue.

In *Case Note 211257* [2009] NZPrivCmr 16, a staff member from a government department dropped a file in an Auckland street. It contained a list with personal information about a large number of individuals. The information was subsequently passed to media outlets. The agency concerned took immediate steps to mitigate the situation and minimise the impact of the incident by:

- getting the original file and copies back, with the assistance of the police;
- seeking and receiving legal undertakings from media outlets that the information would not be published or disclosed;
- notifying the Privacy Commissioner's Office and seeking advice;
- notifying all affected individuals; and
- investigating and taking steps to reduce the likelihood of the situation reoccurring.

Action of this type is what s 113(a) is all about. While the situation was difficult, fast thinking and urgent action to mitigate the breach is likely to keep the situation from falling into the purview of s 118.

Continuing the assessment under s 113, the next step is to consider the sensitivity of that information.

Sensitive personal information

The Act does not define sensitivity. Although some information (for example, that in medical records) is almost always considered to be sensitive, any information can be sensitive in nature depending on the context.

For example, the names and addresses of subscribers to a news magazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be. Following a breach,

Any information can be sensitive, depending on context

Continued on page 11

Photo: BrianAJackson / Contributor / Getty Images

Continued from page 10

an agency will need to determine sensitivity which will require an examination of what personal information has been breached and the circumstances of the breach as well as the potential harms that could accrue to an individual.

In *Case Note 248601* [2013] NZPrivCmr 4, a doctor working in a suburban medical practice had his car broken into and his bag stolen. The bag contained a USB stick holding the personal information of a number of patients. The data detailed the complainant's first and last names and details of prescribed drugs and medical diagnosis/history. The case note outlines the steps the medical practice took in relation to breach and its containment, preliminary assessment, evaluation of the risks associated, notification to affected individuals and prevention of future breaches.

While the Privacy Act 1993 did not declare any sensitive categories of information, it would be a mistake to think the 1993 Act was blind to sensitivities and has been informed by the Australian position. Sensitive information under the Australian Privacy Act is personal information that includes information or an opinion about an individual's:

- racial or ethnic origin;
- political opinions or associations;
- religious or philosophical beliefs;
- trade union membership or associations;
- sexual orientation or practices;
- criminal record;
- health or genetic information; or
- some aspects of biometric information.

This leaves a wide net for consideration under s 113(b).

Actions take since the breach occurred might mitigate the risk

Nature of harm

The next step is to consider the nature of harm that may be caused. This may depend upon the nature of the information and the circumstances of the beach. In providing guidance under Canada's breach notification law, the Privacy Commissioner of Canada has published a set of questions that agencies might consider in relation to possible misuse giving rise to harm.

Some questions you may wish to consider are:

- What happened and how likely is it that someone would be harmed by the information breached?
- Who actually accessed or could have accessed the personal information?
- How long has the personal information been exposed?
- Is there evidence of malicious intent (eg, theft, hacking)?
- Were a number of pieces of personal information breached, thus raising the risk of misuse?
- Is the breached information in the hands of an individual/entity that represents a reputation risk to the individual(s) in and of itself? (eg, an ex-spouse or a boss, depending on specific circumstances)
- Was the information exposed to limited/known entities which have committed to destroy and not disclose the data?
- Was the information exposed to individuals/entities with a low likelihood of sharing it in a way that would cause harm? (eg, in the case of an accidental disclosure to unintended recipients)
- Was the information exposed to individuals/entities who are unknown or to a large number of individuals where certain individuals might use or share the information in a way that would cause harm?
- Is the information known to be exposed to entities/individuals who are likely to attempt to cause harm with it (eg, information thieves)?
- Has harm materialised (demonstration of misuse)?
- Was the information lost, inappropriately accessed or stolen?

Continued on page 12

Continued from page 11

- Has the personal information been recovered?
- Is the personal information adequately encrypted, anonymised or otherwise not easily accessible?

The EDPB has adopted guidance (EDPB *Guidelines on Personal data breach notification under Regulation 2016/679* (2018)) that states in relation to 'Severity of consequences for individuals':

> Depending on the nature of the personal data involved in a breach, for example, special categories of data, the potential damage to individuals that could result can be especially severe, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation. If the breach concerns personal data about vulnerable individuals, they could be placed at greater risk of harm.

Consideration should also be given to the permanence of the consequences for individuals, where the impact may be viewed as greater if the effects are long-term. Undertaking a review of the above, despite the Act falling silent, will significantly assist in determining the nature of harm to be caused under of s 113(c).

The next thing to consider is who got the information?

Recipient or possible recipient

Sometimes a breach is accidental and results in information being sent to the wrong person, but that person diligently returns it to the agency. In other cases, the breach is clearly of malicious intent. Often it is initially unknown whether the information is in the hands of a person with bad intentions or not, and the assumption if the information is in the unknown must be that it is.

The EDPB has adopted guidance (EDPB *Guidelines on Personal data breach notification under Regulation 2016/679* (2018)) that states in relation to 'Severity of consequences for individuals':

> Whether the controller is aware that personal data is in the hands of people whose intentions are unknown or possibly malicious can have a bearing on the level of potential risk. There may be a confidentiality breach, whereby personal data is disclosed to a third party, as defined in Article 4(10), or other recipient in error. This may occur, for example, where personal data is sent accidentally to the wrong department of an organisation, or to a commonly used supplier organisation. The controller may request the recipient to either return or securely destroy the data it has received. In both cases, given that the controller has an ongoing relationship with them, and it may be aware of their procedures, history and other relevant details, the recipient may be considered "trusted". In other words, the controller may have a level of assurance with the recipient so that it can reasonably expect that party not to read or access the data sent in error, and to comply with its instructions to return it. Even if the data has been accessed, the controller could still possibly trust the recipient not to take any further action with it and to return the data to the controller promptly and to co-operate with its recovery. In such cases, this may be factored into the risk assessment the controller carries out following the breach – the fact that the recipient is trusted may eradicate the severity of the consequences of the breach but does not mean that a breach has not occurred. However, this in turn may remove the likelihood of risk to individuals, thus no longer requiring notification to the supervisory authority, or to the affected individuals. Again, this will depend on case-by-case basis.

Consideration should be given to the permanence of the consequences

The Australian eligible data breach scheme refers twice to the possible recipients in its lists of relevant matters to consider as to whether access or disclosure would be likely, or would not be likely, to result in serious harm. It refers first simply to:

> the persons, or the kinds of persons, who have obtained, or who could obtain, the information (Privacy Act 1998, s 26WG(g)).

The second reference is in relation to security technology, and states:

> if a security technology or methodology:
>
> (i) was used in relation to the information; and
>
> (ii) was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information;
>
> the likelihood that the persons, or the kinds of persons, who:
>
> (iii) have obtained, or who could obtain, the information; and
>
> (iv) have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates;
>
> have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology (Privacy Act 1998, s 26WG(h)).

In such cases s 13(d) must be answered in the positive that the unknown person, or known person, will use the information.

Next the organisation must consider what security protects the data that has been breached and if that security is sufficient to protect it?

Security measures

An example of a situation which may fall within s 113(e) is where measures that render personal data unintelligible to any person not authorised to access the data, such as in a bit locker or encrypted file.

The Australian eligible data breach scheme is more specific and directs agencies to consider if the information is protected

Continued on page 13

Continued from page 12

by one or more security measures – the likelihood that any of those security measures could be overcome (Privacy Act 1998, s 26WG(f)). If the recipients of the information are known, or suspected, it may be possible to consider the likelihood of the security measures being effective. This point is made directly in the Australian eligible data breach scheme as follows:

if a security technology or methodology:

(i) was used in relation to the information; and

(ii) was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information; the likelihood that the persons, or the kinds of persons, who:

(iii) have obtained, or who could obtain, the information; and

(iv) have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates;

has obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology (Privacy Act 1998, s 26WG(h)).

If no security measure is in place then s 113(e) will increase the possibility of harm being caused.

Finally an agency must consider s 113(f) and make its final determination.

As s 118 creates an offence, it's important to understand what's expected

Other relevant matters

Under s 113(f) an agency must also consider any other relevant matters. An example might be an aspect of other legislation applicable to the particular agency.

Section 113 is answered in the positive and a report must be immediately made if:

- s 113(a) mitigation has been ineffective and/or any of the below answers are in the positive;
- s 113(b) is positive;
- s 113(c) the nature of harm is possible;
- s 113(d) the person is unknown, is assumed unknown, is unknown at the time of discovery, is untrustworthy or maybe untrustworthy;
- s 113(e) no security, or the security used is breakable, is in place on the data; or
- s 113(f) other factors may be applied.

Failure to report may bring about consequences under s 118, so the rule that has been put forward should be: if in doubt, report.

Lloyd Gallagher is the founder and managing partner of Gallagher & Co and is convenor of the ADLS Technology & Law Committee

A new look at tech and competition law

Hipster antitrust looks beyond traditional economic harm and includes wider effects such as wage inequality, data privacy intrusions and sheer size as grounds to invoke the law

Sasha Daniels

During the past few decades, US regulators' approach to competition law enforcement (or antitrust, as they say in the US) has been largely focused on maximising consumer welfare, frequently measured by the price to consumers.

But a school of thought dubbed 'hipster antitrust' has emerged, focusing on the broader effects of large technology companies on the economy. Hipster antitrust looks beyond traditional economic harm and includes wider effects such as wage inequality, data privacy intrusions and sheer size as grounds to invoke the law.

Like any evolving field, hipster antitrust is unsurprisingly post-modern, flanked by critics espousing the apparent objectivity of a classic or modern approach to the discipline. The hipster antitrust, or new Brandeis movement as it is also known, suggests competition law should look beyond the short-term, narrowly defined consumer welfare standard.

It considers that high concentration in the tech sector gives firms power and influence, not just within relevant markets but in the lives of people more broadly. Of particular interest is the power of large-scale data collection by digital conglomerates, and the effect of AI.

The theory implies that if, for example, Amazon and Alibaba can deliver so many goods at such low prices because of their scale, they must also be able to inflict commensurately huge harm as a result of that scale, and possibly are already. We are just not measuring the harm when we apply traditional competition law.

Somewhat influenced by the hipster antitrust movement, the US Department of Justice, along with attorneys-general representing numerous states, have embarked on broad antitrust action against the likes of Google and Facebook, seeking to break up these tech giants. Results so far have been mixed.

Sasha Daniels

Influenced by the hipster antitrust movement, the US Department of Justice, along with attorneys-generals representing numerous states, have embarked on broad antitrust action against the likes of Google and Facebook, seeking to break up these tech giants

In Australia, the recent Senate Inquiry into Media Diversity considered the impacts on traditional news media of content aggregators of news such as Google and Facebook.

Media outlets argued that Google and Facebook free-ride on necessary investments by media firms and divert revenues away from traditional news media outlets and therefore make media quality and diversity unsustainable. In response, Google and Facebook threatened to either pull their news services from Australia or pull search from the country entirely.

The ACCC's Digital Platforms Services Inquiry 2020-2025 will delve further into understanding the effects digital platforms have on competition.

New Zealand has traditionally followed the consumer welfare standard but has considered total welfare in some cases. Within the merger authorisation context, the Court of Appeal has confirmed that the Commerce Commission can consider public interest benefits and detriments arising from a proposed transaction which go beyond traditional competition indicia. But what will New Zealand's approach to large tech firms be going forward?

Market power

The proposed changes to s 36 of the Commerce Act 1986 could open the door to the application of hipster antitrust in New Zealand.

Firms with substantial market power are prohibited from taking advantage of this for an exclusionary purpose. According to the Cabinet Paper on proposed reforms to s 36, the amendment to the law is intended to prevent firms with market power from harming competition by engaging in conduct such as exclusive dealing, refusal to supply, or predatory pricing. The taking advantage limb of this test has proved challenging for New Zealand regulators and has been out of step with most major comparative jurisdictions.

Government proposes to amend s 36 to prohibit firms with a substantial degree of market power from engaging in conduct that has the purpose, or has or is likely to have the effect, of substantially lessening competition in a market.

The introduction of an effects-based test is seen as making it easier to prove anti-competitive conduct by dominant firms. But what if the breadth of what's considered anti-competitive also expands as a matter of policy? And what if evidence can be led to show an anti-competitive effect is as broad as advocates of hipster anti-trust propose? Might the pendulum swing too far in the opposite direction? Could it become too easy for regulators to take cases against large tech companies and too hard for those businesses to understand permissible conduct, such that innovation in the tech sector might be substantially chilled?

While no new s 36 cases have been prosecuted by the Commerce Commission in more than a decade, and it is not expected that the proposed changes will open the floodgates, the more interesting questions is what a revived s 36 might look like if hipster antitrust took hold among policy makers and regulators in New Zealand?

Sasha Daniels is the lead legal business partner – technology, competition, regulation at Spark NZ and a member of the ADLS Technology & Law Committee ■

ADLS Events

Featured events

Connecting New Zealand Lawyers

New Plymouth sundowner

Wednesday 29 September
The Pepper Room, Millennium Hotel New Plymouth
Waterfront
1 Egmont Street,
New Plymouth
Catering sponsored by MAS

Learn More

Rotorua lawyers' lunch

Thursday 21 October
Ambrosia Restaurant
1096 Tutanekai Street
Rotorua
Sponsored by MAS

Learn More

Newly Suited meet the QCs evening

Thursday 28 October
Stanbeth House
28 Customs Street East
Auckland

Learn More

Central Auckland express lunch

Wednesday 10 November
Glass Goose
78 Federal Street
Auckland
Sponsored by CoLegal

Learn More

Book Here

events@adls.org.nz adls.org.nz

Briefs

Fixed-fee dispute resolution

Lawyers may have clients who are involved in commercial lease disputes as a result of the Covid-19 lockdown and may want to access prompt dispute resolution services. The New Zealand Dispute Resolution Centre (NZDRC) has received a number of inquiries about this.

The government-funded arbitration and mediation scheme for these disputes ends in June 2021. So, NZDRC has launched a special fixed-fee arbitration and mediation service which has been streamlined to ensure parties can access a prompt and cost-effective process, with the fees for these services fixed so they are proportional to the likely amount in dispute.

More to information on the scheme is available **here**

Shock defamation ruling

Australia's highest court has upheld a ruling that makes individuals, media companies and other organisations liable for defamatory online comments, even if they were unaware that the comments had been posted.

In New Zealand, the operators of a social media platform can be held liable as a publisher of defamatory third-party content only if they had been made aware of the offending material and failed to remove it

This means millions of Australians with Facebook and other social media pages can be sued and forced to pay damages to third parties if defamatory comments are posted on their sites.

The High Court of Australia yesterday upheld a ruling by a NSW court earlier this year that said companies and individuals could be held liable because they 'participated' in the publication, even unknowingly.

In New Zealand, the operators of a social media platform can be held liable as a publisher of defamatory third-party content only if they had been made aware of the offending material and failed to remove it (*Murray v Wishart*).

The Australian decision has sparked calls for urgent reform of the country's defamation laws, with critics saying they have failed to keep pace with technology.

The case in question involved Dylan Voller, a former inmate of a youth detention centre.

The defendants were some of the biggest names in Australian mainstream media: Nine Entertainment, News Corp (publisher of *The Australian*) and the parent company of Sky News.

FEATURED CPD

FINAL NOTICE

The Supreme Court's *Bathurst* judgment

CONTRACT
INTERPRETATION
ADMISSIBILITY

Webinar 1 CPD hr
Monday 13 September
12pm – 1pm
Presenter Gillian Coumbe QC, O'Connell Street barristers

Mine (or minefield?) of guidance on contract construction The Supreme Court's highly anticipated judgment in *Bathurst Resources Ltd v L&M Coal Holdings Ltd* [2021] NZSC 85 is out. This webinar will examine two aspects of this important decision. First, all members of the Court have now agreed on the general approach to admissibility of evidence in contract interpretation, and the test for implication of terms. There are, however, some surprises.

FIND OUT MORE

FINAL NOTICE

Cybersecurity: a guide for law firms

RISK
PLAN
MANAGE

Live Stream
1.5 CPD hrs
Tuesday 14 September
4pm – 5.30pm
Presenters Lloyd Gallagher, Gallagher & Co; Arran Hunt, Stace Hammond; Edwin Lim, Hudson Gavin Martin and Campbell McKenzie, Incident Response Solutions

"It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it" – Stephane Nappo.
The risk to cybersecurity is real. You should treat it as a matter of when, rather than if, your firm will be hacked. For many NZ law firms, the once unthinkable has already happened. Our experienced panel will provide practical guidance on what you can do to bolster your defences in the face of faceless, innumerable and ever-inventive enemies.

FIND OUT MORE

FINAL NOTICE

Unit titles: dealing with complexity

COMPLEXITY
GOVERNANCE
DEVELOPMENTS

Live Stream
2 CPD hrs
Thursday 16 September
4pm – 6pm
Presenters Joanna Pidgeon; Thomas Gibbons and Vicki Toan
Chair Liza Fry-Irvine, director, Liza Fry-Irvine Law

Learning outcomes
- Gain a greater understanding of the tensions that can arise between different types of owners and occupiers in unit title developments.
- Learn how to meet governance issues and get top tips for legal compliance and best practice in dealing with practical examples of day-to-day issues.
- Be informed about recent developments in unit titles and body corporate law.

FIND OUT MORE

Breach of mandate & licence fee damages

CONTRACT
TORT
DAMAGES

Seminar | Live Stream
1.5 CPD hrs
Tuesday 21 September,
4pm – 5.30pm
Presenters Matthew Harris, partner, Gilbert Walker and Daisy Williams, barrister, Shortland Chambers

IN PERSON

This seminar reviews the remedies available for breach of an agent's mandate, including in actions for money had and received, an account at equity (for breach of trust), and damages (in contract and tort); and discusses the conceptual basis of licence fee damages and the circumstances in which it is likely to be available.

LIVE STREAM

Class and funded litigation

CONDUCT
CLIENT
RESPONSIBILITY

Seminar | Live Stream
2 CPD hrs
Wednesday 22 September
4pm – 6.15pm
Presenters Paul Collins; Philip Skelton QC; Angela Parlane and Jonathan Woodhams

IN PERSON

Knowing your professional obligations
The rapid growth in class and funded litigation has exposed a range of professional responsibility issues and challenges not encountered in regular litigation and where the Conduct and Client Care Rules do not always fit neatly. This seminar is intended to help lawyers navigate this difficult and potentially perilous field.

LIVE STREAM

The construction landscape amid Covid-19

COVID-19
IMPACT
CONSTRUCTION

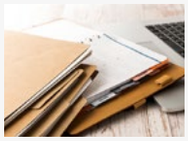
Live stream
2 CPD hrs
Tuesday 5 October
4pm – 6pm
Presenters Geoff Hardy, partner, Martelli McKegg and Shanti Frater, partner, Simpson Grierson

FIND OUT MORE

The impact of Covid-19 on the construction industry landscape is significant. Pandemic restrictions and precautions have seen, and will continue to see, serious and long-lasting implications for current and future construction projects. This seminar outlines the impact of the global pandemic and pandemic-related restrictions on both residential and commercial construction projects, and addresses the various contractual, legal and commercial issues and challenges that have arisen as a result.

CPD IN BRIEF

Criminal disclosure uncovered



Seminar | Live Stream
2 CPD hrs
Thursday 30 September
4.30pm – 6.45pm
Presenters Julie-Anne Kincade QC and Robin McCoubrey, partner, Meredith Connell
Chair Judge Belinda Sellars QC

Disclosure can be fundamental, whether to prove a case or support a defence. Yet it has challenges. The scope for disclosure has widened as technology has developed. Today, counsel needs to consider seeking cellphone provider records of witnesses or social media posts together with more traditional items such as accounting and bank records or fingerprint evidence. Attention must be paid to the independence (or otherwise) of the source and production of evidence. Responsibilities and obligations of counsel can be confusing.

IN PERSON LIVE STREAM

Navigating defective building litigation

In Person | Live Stream
2 CPD hrs
Tuesday 19 October
4pm – 6.15pm
Presenters Andrew Hough; Michael Thornton; Shyrelle Mitchell and Kiri Harkess
Chair Geoff Hardy, partner, Martelli McKegg

New Zealand's building boom over the decades has generated a multitude of claims over poor workmanship. Buildings that remain unrepaired, or are the subject of faulty remedial work, nevertheless continue to be bought and sold. This seminar provides a guide to navigating defective building disputes (from the perspectives of both counsel for plaintiff and defendant) having regard to current issues, and in the context of recent and key case law.

IN PERSON LIVE STREAM

Medically assisted dying

In Person | Live Stream
2 CPD hrs
Wednesday 20 October
2pm – 4pm
Presenters Grant Illingworth QC; Richard McLeod; Dr Jeanne Snelling and Dr Jane Casey

The End of Life Choice Act 2019 comes into force on 6 November 2021. Hear from our panel of lawyers, academics and a psychogeriatrician who will unpack the Act and the corresponding process, offer insights into its implementation, consider capacity and other clinical challenges, and outline some of the uncertainties, red flags and thorny issues.

Chair Professor Kate Diesfeld, Professor of Law, AUT and Chair, AUT Ethics Committee

IN PERSON LIVE STREAM

Evidence law seminar

In Person | Live Stream
2 CPD hrs
Thursday 21 October
4pm – 6.15pm
Presenters Scott Optican, Associate Professor, University of Auckland and Jack Oliver-Hood, barrister

Learning Outcomes

- Update your knowledge of the current versions of key provisions of the Evidence Act 2006 and recent case law on those provisions from the High Court, Court of Appeal and Supreme Court.
- Learn about potential legislative changes to the Evidence Act 2006.
- Gain practical and useful insights into the application of evidence law in civil and criminal cases.

IN PERSON LIVE STREAM

Limitation – A Map for the Minefield

Tuesday 26 October | Webinar | 1.25 CPD hours

Visit adls.org.nz for more information.

WILL INQUIRIES

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 people. If you do not reply within three weeks it will be assumed you do not hold or have never held such a document.

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

reception@adls.org.nz ADLS, PO Box 58, Shortland Street, DX CP24001, Auckland 1140 Fax: (09) 309 3726 (09) 303 5270

COSSEY
Gavin Kenneth

- Late of Auckland
- Machine Operator
- Aged 61 / Died 27'06'21

MARTIN
Robert Leo

- Late of 17 Lynette Place, Mangere, Auckland
- Married
- Worked for Air New Zealand
- Aged 45 / Died 19'08'21

SHORT
David Charles Weir

- Late of 23 St Marys Road, Ponsonby, Auckland
- Aged 57 / Died between 06'08'21 and 07'08'21

LAW FIRM OWNERSHIP OPPORTUNITY

An affordable opportunity for an entrepreneurial lawyer to purchase their own practice. Ideally suited to a young lawyer after a different pace and flexibility, ready to step out on their own, but with an existing client base and law firm structure, without the hassle of starting from scratch.

The current sole practitioner of this virtual/home [Auckland] based law firm wishes to exit for family reasons. They make a good return from minimal hours work. Continue as is for great work/life balance or use it as a base to grow from. The current director could stay connected to the firm as required.

Areas of practice include property, commercial and general practice.

PLEASE EMAIL EXPRESSIONS OF INTEREST TO:
LAWFIRMADVERTISER@GMAIL.COM

Barrister Wanted

A centrally located Chambers has a vacancy for a barrister to share resources with 6 other collegial barristers.

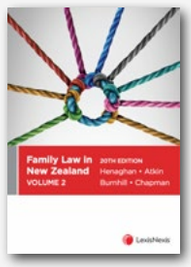
Handily situated in an historic building in Vulcan Lane, you are steps away from major transport links and restaurants and in close proximity to the courts & many of New Zealand's corporate offices.

As well as a spacious office, other facilities include: a Boardroom, library, kitchen, shower and access to all technology. An onsite Office Manager is also available. Very reasonable rates are on offer to the right candidate.

All enquiries to eden@vulcanbuilding.co.nz

COMING SOON

Family Law in New Zealand, 20th edition



Authors Mark Henaghan, Bill Atkin, Shonagh Burnhill and Anna Chapman
Now available to order, due early October.
With in-depth commentary and updated legislation and case law, this book is an invaluable resource for students and practitioners who need an authoritative resource at their fingertips.
Price $136.95 plus GST*
Price for non-members $152.17 plus GST *
(+ Postage and packaging)*
To pre-order this book, please visit adls.org.nz; alternatively, contact the ADLS bookstore by phone: (09) 306 5740, fax: (09) 306 5741 or email: thestore@adls.org.nz.
Please note: While we are under the Level 4 lockdown we cannot process or send out book or hardcopy forms orders. We will process orders when we move back to level 3 or below. Thank you for your understanding.

Chancery Chambers office for rent

Three office spaces are available in the heritage Chancery Chambers building on the corner of Chancery and O'Connell Streets.

- 12.27sqm net located on the fifth floor, internal facing.
- 21.16sqm net located on the fifth floor, consisting of two smaller adjoining offices, internal facing.
- 33.71sqm net located on the third floor of the O'Connell Street side of building.

Opex includes reception to greet clients/receive couriers, kitchen facilities, copy room access and use of shared meeting rooms.

Please contact Krystal Marshall on (09) 303 5277 or krystal.marshall@adls.org.nz for more information