

LAW NEWS

Apr 6, 2023

Issue 10

Inside

■ TECHNOLOGY

How to build a
tech-savvy
law firm

P03-04

■ EVENT

Marie Dyhrberg KC
retires as ADLS
President

P16-18



ADLS

adls.org.nz

Our annual
technology and law

ISSUE

Contents

05

**CYBERCRIME
THREATS
RISK MANAGEMENT**

Why regulating AI is a potential minefield

06

**DEEPAKES
CHATGPT
IDENTITY**

How ChatGPT can enhance deepfakes

07

**CHATGPT
COPYRIGHT
LICENSING**

AI tools spark a raft of litigation

14-15

FEATURED CPD

13, 16-18

EVENTS



Photo: Tomas Anderson / EyeEm / Getty Images

No LawNews next week

LawNews will be taking a break next week for Easter so there will be no issue on 14 April. Our next publication will be on Friday 21 April. We'd like to wish our readers, contributors, advertisers and subscribers a peaceful and relaxing holiday.

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

Reweti Kohere
022 882 2499
Reweti.Kohere@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.

©COPYRIGHT and DISCLAIMER Material from this publication must not be reproduced in whole or part without permission. The views and opinions expressed in this publication are those of the authors and, unless stated, may not reflect the opinions or views of ADLS or its members. Responsibility for such views and for the correctness of the information within their articles lies with the authors.

Cover: William Whitehurst / Getty Images

TECHNOLOGY

Ditch the fax! Tips for building a tech-savvy law firm

No matter how small or large your law firm is, there should be a written contract in place between the firm and the vendor

Edwin Lim

The right technology can help law firms streamline their operations, automate tasks and offer better services to clients.

Examples include practice management systems, document management software, e-discovery tools, legal research tools, billing and invoicing software and video conferencing and communication tools such as Zoom, Teams and Slack.

But choosing the right technology can be time-consuming and daunting. In this article I set out a few factors to consider when procuring technology, based on my experience with our firm that started 15 years ago with eight people and has now grown to almost 50.

Identify your needs

Every firm has unique requirements so the first step in procuring technology is to identify what you need. For example, some firms may want an all-in-one practice management system for their time recording, billing, client relationship and document management. Others may want separate systems to perform some or all of those individual functions.

We use a practice management system that has limited document management capability. As our firm grew, so did the number of documents and emails being created, stored and filed. Rather than trying to find one practice management system to meet all our needs, we decided to implement a separate best-of-breed document management system (DMS) that would work with our existing practice management system. So it's important to evaluate your specific challenges and consider the areas where you want to improve efficiency, reduce costs or enhance client service. Our DMS has helped us to improve in all those areas. If you're not sure where to start, talk to other law firms and ask what solutions they've used, how they've found those solutions and what they might have done differently.

Evaluate the technology

Once you've identified your needs, you should consider the available technology options. Look for solutions that are user-friendly, customisable and scalable. Also consider the level of

Look for solutions that are user-friendly, customisable and scalable

support available from the vendor, as well as the cost of the technology. Take advantage of free or limited-cost trials or demos to test the software before making a purchase. For example, we are upgrading our phone, video conferencing, instant messaging and mobile technology platform and have been trialling a solution for the last few months at no cost to ensure it works.

Evaluate the vendor

When selecting technology vendors, it's important to do some proper due diligence. How long have they been around? Who are their customers? Do they have a decent-sized New Zealand customer base or will you be one of their first local customers?

Look for vendors with experience in working with law firms and a track record of providing reliable and effective solutions. Ask for references from other law firms to get a sense of the vendor's reputation.

Consider integration

Technology should work seamlessly with your existing systems and processes. It's important to consider how it will integrate (eg, practice management systems, DMS, communication and messaging systems, email, calendar) and other software you use, such as accounting or HR software (eg, Xero or MYOB) and standard productivity software (eg, Office 365).

We spend a lot of time ensuring our systems talk to each other. It's equally important to ensure there is a commitment from your vendors to work together:

- when there is a technology project underway;
- to resolve an issue in your technology environment; or
- to ensure the smooth day-to-day operations of all your systems.

Security and compliance

Legal technology often involves sensitive client information so security and compliance are crucial. Remember, you and your firm have obligations under:

- the Lawyers and Conveyancers Act (Lawyers: Conduct and Client Care) Rules 2008 to ensure information remains confidential and to prevent any person from perpetrating a crime or fraud through the firm's practice. The rules specifically refer to taking reasonable steps to ensure the security of and access to electronic systems and passwords; and

Continued on page 04

Continued from page 03

- the Privacy Act, in particular, Privacy Principle 5: when holding personal information, you must have “security safeguards” in place to protect against loss, access, use, modification or disclosure.

Make sure the technology is designed to protect confidential information and ideally meets industry standards for security (eg, ISO27001 and ISO27002, which are international standards and guidelines for information security). Look for technologies with robust security features, such as encryption, multi-factor authentication and access controls.

Training and adoption

The success of a technology implementation depends on user buy-in so before procuring technology, consider how you will train staff to use it effectively.

Ensure the vendor offers training and support to help staff get up to speed quickly. It's also useful for the vendor to train someone in the firm who will provide training to new joiners and others (ie, “train the trainer”).

You should also have a plan for communicating the introduction of the new technology, promoting adoption and encouraging staff to use it consistently. I remember hearing a near-disaster story from someone at another law firm that introduced a new system one Monday but people were told of the change only that morning!

Consider scalability

As your law firm grows, your technology needs may change. It is important to consider the scalability of any technology you procure. You should consider whether it can accommodate your firm's growth and changing needs, and whether it can be easily scaled up or down.

For example, one reason we moved our systems from our physical server room into the cloud about five years ago was to give us the ability to scale up quickly. Previously, to avoid running out of storage space because of the increasing volume of emails and other documents being created, stored or filed, we would have to physically swap out hard drives for larger ones which would result in downtime. Now we simply request our cloud provider to increase storage space and this is done almost immediately.

Read the fine print

No matter how small or large your law firm is, there should be a written contract in place between the firm and the vendor. You should review the contract and be prepared to negotiate it.

Some of the issues to consider in your contracts with your vendor include:

- **Term and termination** Consider the term of the contract and how it can be terminated. If the technology you are procuring is business critical (as opposed to ‘nice-to-have’), you may want to agree an initial term with an automatic rollover for a

We spend a lot of time ensuring our systems talk to each other

similar length term (unless you decide not to continue before renewal occurs).

I've seen contracts that roll over after an initial term on a month-by-month basis, which wouldn't give the firm much certainty that the technology would be available after that initial term. Give yourself plenty of time before renewal to raise any issues with the vendor and negotiate any terms (such as pricing). If you're using technology that is nice-to-have but not business critical, consider whether you want the right to terminate on short notice (eg, 30 days) if you decide the technology is no longer suitable for your firm's needs or if the uptake by people in the firm is not as high as expected.

- **Pricing** Vendors will often provide sharp pricing to get customers onboard. Consider what controls are in place to limit price increases after, say, an initial term. By the time the initial term is up, you're unlikely to be moving to a new system so you don't want to be hit with a significant price increase.
- **Service levels** Consider what levels of service are provided to the firm. How quickly will the vendor respond to a request for support? What is the availability or ‘up-time’ of the service, particularly if it is cloud-based? For example, if you have a time recording solution offered by an overseas vendor, you don't want them carrying out any scheduled maintenance during working hours.
- **Data security/privacy/confidentiality** One of the greatest risks a law firm faces is a security or cyber incident. The contract should set out in detail how the vendor deals with data security, privacy and confidentiality. How quickly will the vendor notify you if it is aware of a data or security breach? Does it even have an obligation to do so?
- **Liability** Check out the vendor's liability position. While it's common for a vendor to exclude liability for indirect and consequential loss, I have seen several legal technology contracts that try to exclude all forms of loss and/or have very low liability caps.
It's common for a vendor and customer to agree that the vendor has unlimited liability (or at least higher liability caps) for all forms of loss for breaches of data, privacy and security as well as the standard carve-outs for breaches of confidentiality, infringement of a third party's intellectual property rights or a wilful breach. However, typically a vendor's initial position is that liability for these events is subject to the general liability cap, not an unlimited or ‘super’ cap, which has to be negotiated.

Conclusion

Procuring technology for law firms requires careful evaluation and planning. By identifying your needs, evaluating the technology options, considering integration and security, planning for training and adoption, evaluating the vendor and entering into a suitable contract, you can select the right technology solution to improve your law firm's efficiency and provide better service to clients. ■

Edwin Lim is a partner at Hudson Gavin Martin, a specialist technology, media and intellectual property law firm ■

TECHNOLOGY

Governments must **tread carefully** in regulating AI

Everything cybercriminals do on social media platforms, emails and even phone calls can be improved with the help of AI



Lloyd Gallagher

Lloyd Gallagher

Artificial Intelligence (AI) has been promoted as the best defence against cyber threats in 2023 but security experts warn the protector might also be used as an attacker.

This has prompted security experts at a recent United States Senate hearing to call for AI regulation which is likely to flow on to Australia and New Zealand. As businesses, consumers and government agencies look for ways to take advantage of artificial intelligence tools and AI threat prevention, experts are warning that AI regulations addressing the challenges facing the technology are needed now, not later.

Cyber risk management is becoming more forward-looking and predictive as it moves from being a typical reactive activity, focusing on risks and loss events that have already occurred, to the rising adoption of advanced analytics and AI technologies.

Predictive risk intelligence uses analytics and AI to provide advance notice of emerging risks, increase awareness of external threats and improve an organisation's understanding of its risk exposure and potential losses.

Cyber threat actors are exploiting this approach by using AI to learn how to evade signature-based systems and developing ways around them.

Attackers have been observed using AI tools to constantly

change their malware signatures, enabling them to evade detection and spawn large amounts of malware to increase the power of their attacks. Using AI, malicious actors can launch new attacks created by analysing an organisation's vulnerabilities through spyware before it is detected.

Manipulating an AI system can be simple if you have the right tools. AI systems are built on the data sets used to train them and making small, subtle changes can slowly steer AI in the wrong direction.

Further, modifying input data can easily lead to system malfunction and expose vulnerabilities. Cybercriminals can use AI to scope and identify vulnerable applications, devices and networks to mount social engineering attacks. AI can easily spot behaviour patterns and identify vulnerabilities on a personal level, making it easy for hackers to identify opportunities to access sensitive data.

Everything cybercriminals do on social media platforms, emails and even phone calls can be improved with the help of AI. For example, creating deepfake content and posting it on social media can propagate disinformation and encourage users to click phishing links and go down rabbit holes that will compromise their individual security.

Spam and phishing emails have used AI to develop

Continued on page 20

The Law Association

ADLS members have voted *in favour* to move forward with a *rebrand* to **The Law Association** Incorporated. ADLS plans to *fully transition* to **The Law Association** by the end of 2023.





TECHNOLOGY

AI and deepfake vocals: whose voice was that?

Are we okay if a long-dead superstar’s voice is used to simulate a new single or a duet with another person who is long gone?

Using this sort of technology, it will probably become easier than before to create a fake version of an interview that seems real



Steven Moe

Steven Moe

Much of the discussion about AI has focussed on ChatGPT and in a recent *LawNews* article I explained how ChatGPT works, with examples of how it could be used [here](#).

But other innovations are showing what AI may be used for and what could become normalised in the future. These new technologies could disrupt how things are being produced.

What does it signal for areas like identity, copyright and art where new technologies allow new ways of creating things? Let’s consider an example involving music and “guest vocalists”.

A famous DJ recently used AI technology to create a new song. David Guetta asked AI for some lyrics in the style of Eminem on a specific topic, then used a voice synthesiser that simulated Eminem’s voice to create a lyric. The song sounds as if it’s a collaboration with Eminem (a link to the [video of it is here](#)).

Guetta had this to say about his process, perhaps being positive and upfront to avoid Eminem becoming upset or pursuing a claim of some kind: “Eminem, bro! This is something I made as a joke and it worked so good, I could not believe it ... I discovered those websites about AI – basically, you can write lyrics in the style of any artist you like. So I typed ‘write a verse in the style of Eminem

about future rave.’ And I went to another AI website that can recreate the voice. I put the text in that and I played the record and people went nuts.”

This raises interesting points because as the technology improves, creators might be able to take samples from famous people and singers, manipulate them and have “guest vocals” that are not in fact the person we might think they are. While this could lead to some interesting collaborations, it also raises some ethical points about identity and manipulation using technology. Are we okay if a long-dead superstar’s voice is used to simulate a new single or a duet with another person who is long gone?

As the creator of a podcast with 340 episodes that each go for an hour, I know my own vocals are “out there” in a very easy-to-access way. Using this sort of technology, it will probably become easier than before to create a fake version of an interview that seems real.

And as the technology improves, how would you feel if you left a short voice message somewhere and it was then used to simulate your voice?

AI raises interesting questions which get at the core of art, identity, creativity and what the limits are – or what they should be. ■

Steven Moe is a partner at Parry Field Lawyers

TECHNOLOGY

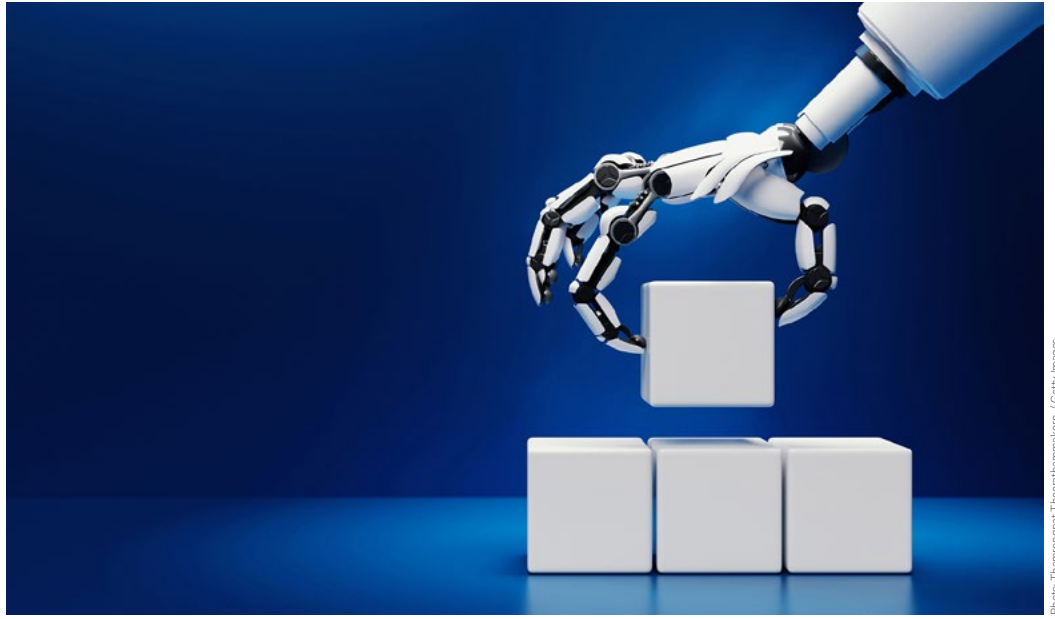


Photo: Thamrongrat Theerathamakorn / Getty Images

Legal challenges mounted against AI tools

To what degree is it permissible for a software tool to look at things it finds online, learn from them and make that derived knowledge available to other users?



Andrew Easterbrook

Andrew Easterbrook

By now, most people will have heard about tools like ChatGPT and Stable Diffusion – AI tools that can generate complex text and images.

They are types of “generative AI”. Unsurprisingly, their release has prompted a raft of litigation based on breaches of rights asserted by content creators. Most of those challenges allege the output appears to be a copy of their work, or occurred because their work was used in training the AI.

There are three major lawsuits targeting AI tools and some have potential implications for New Zealand. As far as we can find, no defendants have filed full responses to the various complaints.

GitHub Copilot

GitHub is a Microsoft-owned code repository, meaning people go there to develop and publish software code. Once published, that code is often subject to licence terms dictating how it may be used. In the not uncommon circumstance that the code is not subject to a licence, GitHub’s **own materials** acknowledge that copyright law does not allow reproduction, distribution or the creation of derivative works.

Open AI and Microsoft collaborated to make a tool called Copilot. Copilot helps people write code, a little like autocomplete on your iPhone. The language model for Copilot was at least partly trained on the GitHub code repository.

In November 2022, lawyers filed a class action lawsuit against Microsoft, GitHub and OpenAI, asserting that:

- Microsoft and OpenAI trained Codex (the language model

used to power Copilot) and Copilot using code published on GitHub;

- doing so violated the open-source licences under which that code had been published; and
- Codex and Copilot output copyrighted materials without following the terms of the relevant licences.

They claim relief on the basis of breaches of copyright legislation, breach of contract, unjust enrichment, privacy and personal data breaches and a range of other causes of action.

Based on previous publications, it is anticipated the defendants will argue that their generative AI system has learnt things by looking at what’s publicly available online and simply use what they learn to create new works (like a human does). They are likely to say that falls within the US “fair use” doctrine, allowing limited use of copyright material. It remains to be seen what defences or arguments may be made in connection with the other causes of action.

Artists vs Stable Diffusion

Stable Diffusion is an online tool that will generate images from text prompts. It is owned by Stability AI.

In January 2023 the same group of lawyers involved in the Copilot litigation filed a second class action on behalf of three artists against Stability AI, DeviantArt and Midjourney. The lawsuit makes similar claims to the Copilot litigation (breach of contract, violation of the DMCA and a few others), and also alleges direct copyright infringement.

Continued on page 21

How worried should lawyers be about ChatGPT?

There is nothing in New Zealand’s legislation that prevents ChatGPT from providing advice in relation to a person’s legal or equitable rights or obligations

Philip McHugh

With the advent of ChatGPT, artificially intelligent bots are claimed to be capable of providing accurate, easily digestible and significantly cheaper legal advice.

How accurate is that assertion? After all, what we lawyers do, provide legal advice, cannot be replaced with artificially intelligent software... right?

ChatGPT itself agrees it is not here to replace lawyers:

Only licensed lawyers are authorized to provide legal advice because the practice of law requires specialized knowledge and training in the law, legal procedures, and ethical considerations. Licensed lawyers have undergone years of formal education and training in law schools, passed the bar exam and are subject to ongoing ethical and professional obligations to their clients and the legal profession.

Providing legal advice involves interpreting complex legal principles and applying them to specific situations, which requires a deep understanding of the law and legal system. Licensed lawyers are also bound by professional standards of conduct and ethical rules that ensure they act in their clients’ best interests and maintain the confidentiality of their clients’ information.

By requiring only licensed lawyers to provide legal advice, the legal system seeks to ensure that people receive accurate and reliable information about their legal rights and obligations. This helps to prevent the unauthorized practice of law and ensures that legal services are provided by trained professionals who are accountable to their clients and the legal profession.

So, there it is. A complete explanation, straight from the horse’s mouth, as to why AI cannot replace lawyers. Lawyers are safe; their jobs are secure and will always remain so.

Hold on. Is there any legislative justification for ChatGPT’s position? Well, again, according to ChatGPT, there is. You see,

What would happen if a law firm used a white label version of ChatGPT to sit behind its website chatbot?

“in most jurisdictions, the practice of law is regulated by law societies or bar associations that are established by legislation”. Very true. ChatGPT continues, “the unauthorised practice of law is prohibited by law and can result in both civil and criminal penalties”.

When asked specifically whether ChatGPT’s opinion holds true in New Zealand, I get the assertion that “only licensed lawyers are authorised to provide legal advice” in New Zealand. When asked to justify that assertion, ChatGPT states that “the practice of law is regulated by the New Zealand Law Society, which is established by legislation, specifically the Lawyers and Conveyancers Act 2006.

Under New Zealand law, it is illegal for a person who is not a licensed lawyer or authorised under the Lawyers and Conveyancers Act to provide legal advice or services to the public.”

Well, this is not quite accurate. The Lawyers and Conveyancers Act 2006 makes it an offence only if a person, who is not a lawyer, provides legal services in New Zealand and describes themselves as a lawyer (note the word ‘and’).

The fine print

You will note that I switched from referring to lawyers providing legal advice to lawyers providing legal services. The Act uses the term ‘legal services’ and the definition of legal services is much broader than the provision of advice in relation to any legal or equitable rights or obligations (ie, ‘legal advice’).

Under the Act, if a person makes it clear he or she is not a lawyer, the Act cannot be used against them if they provide a wide swathe of legal services (excepting work of a kind defined as being a reserved area of work – effectively, court work). That person, or artificially intelligent software, would not have contravened the Act because they would not have undertaken

Continued on page 09

Continued from page 08

an unauthorised practice of law though they may have given legal advice.

Well, there you have it. There is nothing in New Zealand's legislation that prevents ChatGPT from providing advice in relation to a person's legal or equitable rights or obligations. When prompted, ChatGPT is careful to be clear about what it is providing, though.

When I asked ChatGPT why its answers to my questions are not considered legal advice, it responded with:

My answers to your questions are not considered legal advice because, as an AI language model, I am not a licensed lawyer and I do not have the authority to practice law or provide legal advice. While I can provide information and general guidance on legal topics based on my knowledge and training, I cannot offer legal advice tailored to your specific circumstances, nor can I provide you with legal representation in a court of law.

It is important to note that legal advice requires an understanding of the specific facts and circumstances of a particular case or situation, as well as an analysis of the relevant laws and legal principles. This is why legal advice is typically provided by licensed lawyers who have undergone specialized education and training in the law, and who are authorized to practice law and provide legal advice under the laws of their jurisdiction.

Therefore, while my answers may provide general information and guidance on legal topics, they should not be relied upon as a substitute for legal advice from a licensed lawyer in your jurisdiction. If you have specific legal questions or concerns, you should consult a licensed lawyer who is authorized to practice law in your jurisdiction.

Somewhat circular, and ChatGPT had to be prompted to provide that caveat.

If I just asked it legal questions, such as 'what duties does a trustee have?', 'what liability does a trustee have?' and 'can you give me an example of a breach of fiduciary duty?', it provides a cogent, sensible and accurate answer, along with a good example (though it took a relatively long time to provide the example – it clearly had to think). As long as ChatGPT does not rename itself to LawyerGPT, no foul has been committed.

There is, of course, concern in having an artificially intelligent piece of software provide information and general guidance to any person who may ask it questions about a legal or equitable right or obligation, particularly when that artificially intelligent piece of software makes an output that appears cogent, is easily digestible and, most importantly, for a lot of people at least, is free.

Nobody is going to alter their position in reliance on answers given to it by ChatGPT, are they? Perhaps not – likely not if they know it's ChatGPT giving the answers and is more likely to create the 'Dr Google' effect for lawyers.

But what would happen if a law firm (or an accounting firm) used a white label version of ChatGPT to sit behind their website chatbot? Or a community law hub? A business advisory? An employment advocate? Amazon? Facebook? ■

Philip McHugh is a solicitor at Grayson Clements Ltd ■



Document Analysis Review Tool

AI-Powered eDiscovery and Investigations

Incident Response Solutions (IRS) is a specialist forensic technology firm, delivering Electronic Discovery Reference Model (EDRM) services.

We have expanded our suite of review EDRM tools to include **Reveal**, a leading cloud-based artificial intelligence resource. IRS has also created its own 'Document Analysis Review Tool' (DART), leveraging the Reveal cloud-hosted platform to assist lawyers in the efficient review of documents.

Examples of where our clients may use Reveal and DART include investigations, eDiscovery and privacy breaches matters. Whether your case is routine or a complex tailored discovery, we will assist you using a combination of Reveal with its configurable AI models and our extensive forensic experience.

DART kick-starts your review by prioritising relevant documents, so you can immediately focus on what is most important first. As you review, the Reveal AI model then conducts 'continuous active learning' to ensure you are being presented with a batch of documents that are more likely to be responsive. Reveal and DART then produce reports to ensure Courts and interested parties have independently verifiable discovery methodologies and results.

Examples of Reveal's pre-trained AI models include privilege reviews, fraud, bribery, kickbacks, bullying, sexual harassment and discrimination. IRS can also assist with customised AI models, including our pretrained 'New Zealand Privacy Breach' offering, and more specialised fraud, cartel conduct, M&A and other subject matters.

Reveal and DART are tools that not only save on cost and time, but also promote efficiency and consistency.

"The partnership between Incident Response Solutions in New Zealand and Reveal is an exciting development, as Incident Response Solutions take full advantage of the end-to-end, cloud-based Reveal 11 platform and AI models to enable their Privacy Search Tool" – Wendell Jisa, founder & CEO of Reveal

Now is the time to engage these leading EDRM services. To get started, contact us to discuss your requirements.

Incident Response Solutions
0800 WITNESS (0800 948 637)
support@incidentresponse.co.nz
41 Shortland St, Auckland

New Zealand likely to face international pressure to toughen privacy laws

As international privacy laws become more robust and penalties for non-compliance increase dramatically, businesses need to be aware of the potential implications for their operations when operating across borders

Amy Kingston-Turner

As businesses rely increasingly on data, technology and digitisation, the importance of cybersecurity and privacy cannot be overstated.

While New Zealand has not yet experienced a wholesale reworking of its privacy laws, as has occurred in Europe, Australia and California, Kiwi businesses must be proactive in managing cybersecurity risks, especially given the recent developments in international privacy laws.

Many international privacy laws have extraterritorial application so New Zealand businesses must be aware of potential implications for their operations, especially as laws become tougher and penalties increase.

For example, a wholesale review of Australia's Privacy Act 1988 (Cth) is underway, with recommendations to make it more robust, including a widening of the definition of "personal information" and the removal of the small business exception.

These recommendations come on top of recent changes that broadened the extraterritorial reach of the Privacy Act and increased fines to the greater of A\$50 million, three times the value of the benefit attributable to the breach or 30% of the company's adjusted turnover during the breach period.

These most recent changes were hurried through the Australian Parliament at the end of 2022 in response to the Optus and Medibank data breaches. This demonstrates the seriousness with which governments are taking privacy breaches and New Zealand businesses need to be aware of the potential consequences of non-compliance.

While most New Zealand businesses were not directly affected by the changes the General Data Protection Regulation (GDPR) brought to the privacy landscape, it is unlikely that we can ignore the changes happening in Australia. New Zealand businesses operating in or planning to enter Australia will need to be mindful of any changes to Australian privacy laws and how they may impact their operations. As penalties become more severe, businesses can no longer afford to treat cybersecurity and privacy as a secondary concern.

In light of the changes happening in Australia and around the world, New Zealand is likely to face international pressure to review its own privacy laws, particularly if it wants to continue to position itself as a trusted trading partner on the world stage.

This may become more urgent as New Zealand seeks to maintain its "adequacy" status under the GDPR. The message is clear: businesses need to start taking privacy and cybersecurity seriously now, both to comply with the requirements of existing local and international laws and to prepare for the potential changes that are yet to come.

Here is a simple checklist of practical steps businesses can take now to comply with data protection laws and reduce the risk of a cyber breach:

- Appoint a privacy officer;
- Map your data/personal information to give you the information you need to understand what further compliance obligations you have;
- Draft and publish a privacy policy;
- Put in place reasonable security measures;
- Create a process to identify and respond to data breaches.
- Collect personal information only for a lawful purpose;
- Figure out which laws apply to the personal information and whether you are a controller or processor under these laws;
- Create a process to respond to requests;
- Create a process for deleting personal information you no longer need;
- Manage data transfers correctly;
- Start conducting privacy transfer impact assessments;
- Train your staff on best practice when dealing with personal information; and
- Review and update all policies and documents on a regular basis (eg, annually) to ensure ongoing compliance with privacy laws.

New Zealand businesses must take cybersecurity and privacy seriously to remain competitive, both locally and internationally. As international privacy laws become more robust and penalties for non-compliance increase dramatically, businesses need to be aware of the potential implications for their operations when operating across borders. As privacy laws continue to evolve, businesses must remain vigilant and adaptable to ensure they can operate in a changing regulatory environment. By prioritising cybersecurity and privacy, businesses can protect themselves, their customers and their reputation and ensure their long-term success. ■

Amy Kingston-Turner is a director at Source Law Ltd ■



Amy Kingston-Turner

Why **global standards** are needed to oversee AI

Artificial intelligence can identify patterns unseen to the human eye, learn, and make predictions about individuals and groups, as well as create information that would not have otherwise existed.

Vaheeni Naidoo

Artificial intelligence (AI) has vastly improved the manner and capability in which we do things. Research shows more than half of companies globally, especially in emerging nations, have adopted AI in at least one function. It is used in all sectors, from optimising service operations through to recruitment, and its functionality is extending to the capture of biometric data, judicial systems and finance.

So, AI is making key decisions in people's lives. But while it brings multiple advantages, the technology poses both risks and challenges. It is therefore imperative to consider the ethical implications which the use of AI poses.

AI is the technology which gives a machine or a digital computer the ability to execute tasks performed by humans, such as thinking and learning. However, it emanates from programs and algorithms generated by humans. These analyse, disseminate and study information effectively, whilst algorithms follow the programmed rule-set used in calculations and other problem-solving operations. Thus, some of the ethical issues surrounding the use of AI stem from the fact that AI is crafted by human programming.

But there are no global laws overseeing AI, its development and usage, leaving the ethical aspects of AI usage unclear.

Globally, there are discussions about the under- and over-regulation of AI, both of which pose ethical concerns. Whilst there are several legal guidance aspects around consent and appropriately informing users, the legal interpretation and practical implementation of requirements, such as AI fairness, are still in their development stages. Essentially, there is no one-size-fits-all approach for assessing trustworthy AI principles.

Discrimination and bias

Artificial intelligence bias is regarded as the underlying prejudice upon which AI is created. It can lead to discrimination and other social impacts, heightening ethical concerns. Both human bias and resulting discrimination can be replicated when programs or algorithms are developed.

According to *Harvard Law Review*, when the integration of bias and discrimination is applied at a scale in sensitive application areas, the situation can worsen. For example, in some instances algorithms determine which prisoners should be granted parole, which sectors of the public should be afforded

Essentially, there is no one-size-fits-all approach for assessing trustworthy AI principles

housing opportunities and so forth. In some instances, the output of AI can be regarded as replicating bias and discrimination which are already prevalent in society.

Since 2019, the Dutch government has been involved in the highly publicised scandal about the self-learning algorithm through which the tax authorities detect fraud in respect of those applying for childcare benefits. Families were penalised on a mere suspicion of fraud, based on an algorithm, and thousands were plunged into poverty. Some committed suicide whilst several children were incorrectly placed in foster care.

Privacy

Artificial intelligence can identify patterns unseen to the human eye, learn, and make predictions about individuals and groups, as well as create information that would not have otherwise existed. Inferring information in this manner challenges not only the definition of personal information but also raises privacy aspects as to whether it is acceptable to infer personal information about an individual who could have chosen not to disclose it.

Collecting data via AI also raises privacy issues, such as whether informed consent is freely given, whether the holder of information can opt out, whether the data collection can be limited and whether it can be deleted on request.

The ultimate question remains as to whether an individual would even be aware that their data had been collected, which would allow them to make a reasonably informed decision as to the next steps about its retention.

Even when data is publicly available, the use of such data can breach what is referred to as **textual integrity**. This fundamental principle in legal discussions of privacy requires that an individual's information is not revealed outside the context in which it was originally produced.

Continued on page 21

Government ramps up moves on consumer data rights

The CDR aims to create a fairer and more competitive marketplace by allowing consumers to share their data in almost any way they wish

Luke Han

In 2020, the government announced plans to introduce consumer data right (CDR) legislation, a regulatory framework giving consumers greater control over their data and enabling them to share it with various third-party providers.

The CDR is already in place in Australia, where it has been used to give consumers more choice and control of their data in sectors such as banking and energy.

Our government is now consulting on the design and is expected to introduce legislation this year, after circulating a draft bill for feedback and consultation. Once the legislation is passed, the CDR is likely to be introduced first in the banking sector, with others to follow.

The CDR aims to create a fairer and more competitive marketplace by allowing consumers to share their data in almost any way they wish. This could include sharing data such as transaction history, account balances and product preferences.

We expect the CDR to have several benefits for consumers, allowing them:

- **Greater control over data** Consumers will have greater control over their personal data and will be able to decide who can access it and for what purpose;
- **More choice** The CDR will give consumers more choice in the marketplace, allowing them to compare products and services more easily;
- **Better deals** Increased competition could lead to better deals and lower prices for consumers; and
- **Improved transparency** Consumers will have greater visibility over how their data is being used and who is using it.

Cabinet paper

One of the more recent updates by the government is a Cabinet paper published late last year, *Further decisions on the consumer data right*.

Amongst other things, the paper confirms various 'floating' topics.

Penalties

These are categorised into four tiers.

Tier 1 relates to infringement notices of up to \$20,000 and infringement offences of up to \$50,000. MBIE provides examples of what would constitute a tier 1 breach, such as failure

to maintain transaction records or breach of notification or disclosure requirements.

Tier 2 relates to penalties for bodies corporate and individuals. For a body corporate, there is a possibly pecuniary penalty of up to \$600,000 and for individuals a pecuniary penalty of up to \$200,000. Examples of a tier 2 breach include failure to meet reporting requirements, failure to have adequate internal complaint processes, and authentication and identity check failures.

Tier 3 also relates to bodies corporate and individuals and specifies higher thresholds of penalties. A higher level of breach that may be included in tier 3 includes misleading or deceiving a person into believing something that may actually be invalid relating to CDR data or a CDR consumer.

Tier 4 is the highest tier and relates to penalties of up to \$5 million or greater. This is to capture serious breaches such as a person knowingly, intentionally or recklessly misleading or deceiving another person in relation to CDR or fraudulently holding out false accreditation.

Relevant sectors

The government wants the banking sector to be the first to be assessed and captured under the CDR legislation. It says any standards from CDR legislation would likely build on existing standards in the industry, such as those developed by Payments NZ's API Centre that relate to the concept of open banking. An intimate level of consultation will be necessary to match and compare these standards with the relevant legislative requirements.

Governmental roles

Finally, the Cabinet paper has confirmed MBIE's role as the overseer and administering department for developing CDR. The Commerce Commission will enforce the relevant CDR rules and the government has detailed an extensive list of enforcement powers that could be available to the commission.

Privacy will still remain in the remit and jurisdiction of the Office of the Privacy Commissioner but certain requirements under the Privacy Act may apply in parallel to potential CDR obligations. MBIE is specifically considering the application of relevant privacy principles on CDR obligations. ■

Luke Han is a solicitor at MinterEllisonRuddWatts ■

ADLS Events

Featured events

Connecting New Zealand lawyers

Hamilton Express Lawyers' Lunch

Wednesday 19 April
12.30 – 2pm
The Bank Bar & Brasserie
(Garden Bar),
117 Victoria Street,
Hamilton Central



[Learn more](#)

Wellington Express Lawyers' Lunch

Wednesday 10 May
12.30 – 2pm
Dirty Little Secret,
54 Taranaki Street,
Te Aro, Wellington



[Learn more](#)

Newly Suited Fark Knows Quiz Night

Wednesday 17 May
5.30 – 7.30pm
Coops Corner Pub,
204 Quay Street,
Auckland CBD



[Learn more](#)

Upcoming

May

ADLS Annual Employment Law Dinner

June

North Auckland Express Lawyers' Lunch
Tauranga Express Lawyers' Lunch

GROVE
DARLOW
& PARTNERS

Solicitor – Commercial Litigation Auckland CBD Minimum of 2 years' PQE

For almost 40 years our firm has developed and maintained a position at the premium end of the legal profession, providing specialist legal advice and counsel in civil litigation and commercial transactions.

Our lawyers are all highly experienced, providing litigation and strategic advice to our commercial clients nationally and internationally. Our client base includes financial institutions, construction firms, manufacturers and distributors, travel companies, Māori commercial entities, body corporate and property management companies, accounting, and business advisory firms. We have a proud record of robust and effective litigation and commercial practice.

We offer candidates an exceptional working environment, autonomy, and an ability to spend time on their feet in court. The work is diverse, highly commercial, complex, challenging, and well suited to individuals who look to make a meaningful contribution to the matters they work on.

If you:

- wish to further your skills as an advocate
- have an excellent academic record
- genuinely love being a litigation lawyer and enjoy having client contact
- are interested in working on a wide range of commercial litigation
- are wishing to develop your own litigation practice

Please email your application, including cover letter, CV and academic transcript to:
mareec@grovedarlow.co.nz

FEATURED CPD

Sexual violence legislation updates

CRIMINAL
ALL LEVELS
SEMINAR



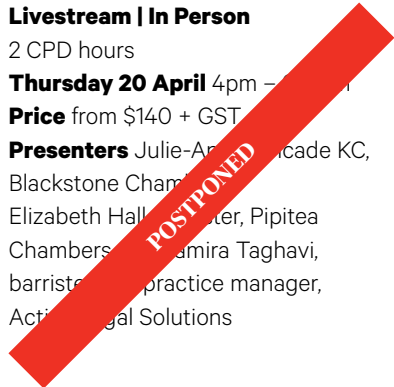
Livestream | In Person

2 CPD hours

Thursday 20 April 4pm – 6pm

Price from \$140 + GST

Presenters Julie-Anne [redacted] KC, Blackstone Chambers, Elizabeth Hall [redacted], Pipitea Chambers, Samira Taghavi, barrister, practice manager, Act [redacted] Legal Solutions



► The changes to the Evidence Act 2006 introduced by the recent amendments to the Sexual Violence Legislation Act 2021 were controversial and are significant. Criminal defence lawyers must understand the implications of these changes and how to deal with them.

... IN PERSON

... LIVESTREAM

Work IT systems: how private is your personal information?

PRIVACY
ALL LEVELS
WEBINAR



Webinar 1.25 CPD hours

Wednesday 26 April

12pm – 1.15pm

Price from \$100 + GST

Presenters Mihai Pascariu, partner, Hamilton Locke and Jennifer Murdoch, solicitor, Hamilton Locke

► The webinar addresses the question of whether personal information on your work IT system remains private. It covers the practical ramifications of recent privacy decisions in New Zealand and overseas jurisdictions for both employees and companies, how personal information may be misused, the acceptance of the tort of “intrusion upon seclusion” in New Zealand and what a privacy policy should address to ensure adequate protection.

... FIND OUT MORE

The Annual Property Law Conference 2023

PROPERTY
ALL LEVELS
CONFERENCE



In Person | Livestream

4.5 CPD hours

Thursday 27 April

12.30pm – 5.30pm

Price from \$400 + GST

Chair Tony Herring, partner, Gibson Sheat Lawyers

► One of the leading property law conferences in New Zealand, this offers a unique opportunity for legal professionals to engage, connect and learn from the best minds in their area of practice. The programme is curated to give practical insights and guidance on key aspects of property law.

... IN PERSON

... LIVESTREAM

Ready, set, retire! Crafting succession and a lifestyle change

ALL LEVELS
ADVANCED
SEMINAR



In Person | Livestream

2 CPD Hours

Tuesday 16 May

4pm – 6.15pm

Price from \$140 + GST

Presenters Don Thomas QSM; Janine Roberts and Carmel Byrne

► So, you want to retire or have a change of lifestyle? Where do you start? Do you have succession options? Drawing on the experience of two lawyers, an accountant and a career coach, this seminar will arm you with practical information and insights to take you from 'what if' to 'made it'.

Chair John Hart, barrister, John W Hart Limited

 **IN PERSON**

 **LIVESTREAM**

Cradle to Grave™ 2023

GENERAL PRACTICE
ALL LEVELS
CONFERENCE



In Person

Christchurch & Auckland

Livestream

7.5 CPD hours

Monday 22 May &

Thursday 25 May

8.15am – 5.15pm

Price from \$600 + GST

Chair Bill Patterson

► Cradle to Grave™ is the flagship conference for general legal practitioners as well as those working in the areas of property, family law, trusts, taxes, wills and estate planning. The Cradle to Grave™ conference offers a unique opportunity to engage, connect and learn from the best legal minds in your area of practice. In-person conference includes networking from 5.15pm.

 **FIND OUT MORE**

Leading your career

WOMEN
INTERMEDIATE
WORKSHOP



In Person

8 CPD hours

Auckland

Thursday 8 June

8.45am – 5pm

Price from \$980 + GST

Facilitators Miriam Dean KC and Liz Riversdale

► This practical, interactive one-day workshop will arm you with resources, self-confidence and focus to apply immediately to your role and enhance your future career. The workshop will be followed by a networking event from 5pm.

 **FIND OUT MORE**

Full house farewells ADLS President Marie Dyhrberg KC

On 29 March, an uncharacteristically cold autumn night in downtown Auckland, members of the judiciary and the legal profession crammed into the rooftop bar of the So/Auckland hotel to honour outgoing ADLS President, Marie Dyhrberg KC.

After three years at the helm – the maximum time a president can hold office under ADLS’ rules – and two terms on the ADLS Council, Dyhrberg was bowing out, handing over the reins to fellow councillor Tony Herring.

Chosen to welcome Dyhrberg that night and comment on her contribution to the profession was former High Court judge Dame Judith Potter, who described Dyhrberg as a “natural leader” with the empathy that enabled her to “work with and for the benefit of the full range of humankind”.

Her ADLS presidency had been “remarkable” and “outstanding”, Dame Judith, a former ADLS president herself, said. “You are, quite simply, a taonga.”

Not only had she held office during a critical period in the development of ADLS, but during that time Dyhrberg had also been a valuable member of a Heads of Bench group, set up by the chief justice and chaired by Chief High Court Judge Susan Thomas to ensure the courts operated efficiently and safely during covid and continue to address the more recent challenges caused by flooding.

Dame Judith noted that Dyhrberg had also served as convener of the ADLS Criminal Law Committee for 15 years and was a member of the ADLS Parole Committee. This was “a huge contribution”, Dame Judith said, which Dyhrberg, as a leader of the criminal bar, had made “so ably and comprehensively”. In addition, she had been a mentor to newly appointed and admitted barristers for the past 35 years, with a particular focus on south Auckland, where Dyhrberg was hugely respected. She was the first female chair of the International Bar Association’s criminal law committee and the first woman president of the Criminal Bar Association.

As a leader of the defence bar, Dyhrberg had served the public and the judicial system with “outstanding ability, courage, wisdom, empathy and at all times utter professionalism”, Dame Judith said.

“I can say from first-hand experience that when Marie appeared as counsel before me in the High Court, as she did on so many occasions in the 15 years that I was sitting, I could and did trust absolutely her integrity and her honesty. Counsel who consistently offer those attributes make a significant impact and contribution to the judicial process. It was always a pleasure to have Marie appearing.”

Jenni McManus



Marie Dyhrberg KC



Emma Priest, Rachael Reed KC and Judge Belinda Sellars KC



Judge Gerard Winter, Judge Jonathan Moses and Justice Simon Moore



Justice Gerard van Bohemen, Barbara Hunt and Gary Gotlieb



Julie-Anne Kincade KC, Judge Stephen Bonnar KC, Dame Judith Potter and Samira Taghavi



Justice Susan Thomas, Judge Anna Fitzgibbon and Raynor Asher KC



Catherine Stewart, Matt Casey KC and Joanna Pidgeon



Rachel Oldham-Ormiston and Tim Jones



Marie Dyhrberg KC, Dame Judith Potter and Julie-Anne Kincade KC

Continued on page 18



Marie Dyhrberg KC and Jim Farmer KC



Richard Chen, Michael Wallmannsberger and Andrew Simpson



Judge Jonathan Moses and Raynor Asher KC



Justice Simon Moore, Gary Gottlieb and Justice Graham Lang



Bernard Smith, John Hickey and Joanna Pidgeon



Kristin Sumpter, Rachael Reed KC and Dame Judith Potter

Offices Available

Following some barristers retiring, we have three offices of varying sizes available for rent.

The Chambers share a refurbished floor (with separate areas) with Hussey & Co., a boutique forensic and general accounting firm. There are shared meeting rooms (a formal boardroom with video conferencing facilities and a less formal meeting room), and communal entrance and client waiting area.

Telephones, internet connection, printing and secretarial services also available and some furniture available.

Cost depends on office size and range from \$150 – \$300 per week plus gst. No long-term commitment required.

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

Contact: [Shane Hussey](mailto:Shane.Hussey@hco.co.nz) for further details, Shane@hco.co.nz
09 300 5481

Advertise your business

Get your message in front of our readers comprised of nearly 6,000 lawyers, judges, politicians and academics.

Contact our account manager Darrell Denney
M 021 936 858
E darrell.denney@adls.org.nz

LAW NEWS



RELIEF CORONER

Applications are invited from persons wishing to be considered for appointment as a full-time relief coroner. Appointment will be for a three-year term. Location is negotiable.

Relief coroners are appointed under section 104 of the Coroners Act 2006. The role of coroners is to establish when, where, how and why a death happened, and also to determine whether anything can be done differently that might prevent similar deaths in the future.

To be appointed as a relief coroner the Act requires that you must have held a practising certificate as a barrister or solicitor for at least five years.

A position description and application forms are available from the Ministry of Justice website [here](#).

The close-off for expressions of interest is 4pm
21 April 2023.



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

KALOMAKAEFU

Pomilo

- Late of 164A Hendon Avenue, Mount Albert, Auckland
- Widower
- Retired
- Aged 78 / Died 06'03'23

PATUKI

Gavin Kanongataa Sehina

- Late of Cranmere Crescent, Mangere, Auckland
- Married
- Welder
- Aged 52 / Died 19'02'23

Business For Sale

Reputable Law Firm | Proven & Profitable

\$\$\$

Bay of Plenty

This well-established law firm has a loyal and extensive client base throughout New Zealand, with a strong and desirable position in the Bay of Plenty region. Offering a variety of legal services led by a highly skilled team of lawyers, this firm has built its reputation on honesty, integrity, and excellence.

Acquiring this reputable business presents a unique opportunity to expand within the legal industry while generating significant revenue and profit.

- Long-standing & esteemed law firm
- Great location & community support
- Diverse services, qualified lawyers
- Loyal clientele, respected reputation

Steve Catley 021 341 117
steve.catley@linkbusiness.co.nz



LINK

0800 546 528
LINKBUSINESS.CO.NZ

Continued from page 05

sophisticated emails that are indistinguishable from the real thing. Recent AI learning has seen Microsoft Azure and T-Mobile come under constant attack, with several successes for threat actors.

Cyber threats are increasing through ransomware attacks, commodity malware and heightened dark-web enablement. Interpol reports the projected worldwide financial loss to cybercrime for 2021 is US\$6 trillion, twice as much as in 2015, with damages set to cost the global economy US\$10.5 trillion annually by 2025.

Globally, leading tech experts report that 60% of intrusions incorporate data extortion, with a 12-day average operational downtime due to ransomware.

The concerns reached the European Union in April 2021, prompting the first published proposal for regulation on artificial intelligence.

The US Chamber of Commerce on 9 March 2023 also called for regulation of AI technology to ensure it does not hurt growth or become a national security risk. New Zealand has heard the call and in February 2023 began work on regulating AI by incorporating AI rules into **existing legislative frameworks**.

However, most of the existing laws focus on privacy

collection, data protection and data sharing, leaving much of the development of technology under standard business ethics, which we have seen to be largely lacking. But how far should we regulate? And will regulation create a reduction in invention?

Arguably, regulation is needed to prevent mischief but the lack of understanding by legislators is likely to lead to poor legislation. It is suggested a risk-based approach may be the best to balance issues with rights, but the regulation is still developing.

No matter what happens, AI is here to stay and government officials must recognise the industry has led the development of this technology and endeavoured at self-regulation for a long time. Working with companies to find reasonable protections for privacy and other concerns is paramount in maintaining trust and safety between society, government and industry.

Such collaborative efforts ensure the best possible practices are established. Otherwise, society risks creating policies that allow unconscious bias within algorithms, loopholes within otherwise acceptable business cases that allow for abuse and misuse by third-party actors and other negative unforeseen consequences associated with AI technology. These actions will erode societal trust in the technology as well as in the institutions that are meant to serve and protect it. ■

Lloyd Gallagher is the managing partner at Gallagher & Co Consultants ■

Using AI, malicious actors can launch new attacks created by analysing an organisation's vulnerabilities through spyware before it is detected



ADLS CPD

Thursday 8 June 2023
8.45am – 5.00pm
8 CPD Hours | Workshop
Networking 5.00 - 6.00pm

Leading Your Career

Plot your path to success. Let one of New Zealand's top barristers and leadership experts Miriam Dean KC arm you with the resources, self-confidence, and focus to immediately apply to your role and enhance your career in 2023 and beyond.

Book Now

Continued from page 07

Stable Diffusion and DreamUp [the DeviantArt generator] was trained on a public dataset of 400 million images and captions. The lawsuit claims that training the tool in that way infringed artists' copyright, and enabling the reproduction and distribution of derivative works based on those images is also copyright infringement.

Getty Images vs Stable Diffusion

Getty Images, a stock photography company, has also sued Stability AI, both in the UK and in the US. The claim is that Stability used copies of Getty's images to train its AI model and at times produces images that are highly similar and derivative of the Getty Images library and frequently include something that looks like the Getty Images watermark.

In January, Getty Images announced it commenced proceedings against Stability AI in the UK on the basis of copyright and "other intellectual property rights". The UK has a "fair dealing" exception to copyright law (narrower than the US "fair use" doctrine and more similar to our own), and has specific exemptions from copyright for "text and data mining" for non-commercial research.

In February Getty Images filed a complaint in the US making claims for breach of copyright, trademark and unfair competition laws.

Continued from page 11

In such instances, the traditional definition of privacy would not be technically or legally practical, nor particularly helpful as an effective way to protect the privacy of individuals. With the lack of general regulation about AI, privacy cases are dealt with in an individual manner based on country-specific regulation.

At the end of 2021, the Office of the Australian Information Commissioner found that Clearview AI had violated the Australian Privacy Act, based on the collection of images and biometric data without the consent of data holders. A joint investigation was concluded with Australia's OAIC and the UK's ICO, which confirmed its intention to impose a potential fine of more than £17 million. This was supported by three Canadian privacy authorities as well as France's CNIL which ordered Clearview AI to stop processing and to delete the data.

Plagiarism

Recently, plagiarism concerns surrounding ChatGPT have been widely published in the media. The AI chatbot, released in November 2022, uses natural language to enable a normal conversation that is humanlike.

ChatGPT can provide responses to questions, content for essays and compose articles. Concerns emanating from ChatGPT relate to whether the information will be used in an

The issues

These lawsuits centre around one main issue: to what degree is it permissible for a software tool to look at things it finds online, learn from them, and make that derived knowledge available to other users?

The two strongest legal challenges seem to be in contract law ("you trained your model on data obtained through breach of contract") and copyright ("training your model on my art is a breach of copyright"). The copyright claim, in particular, is likely to turn heavily on the American concept of "fair use" and whether that provides a defence, and the UK's text and data mining exemption.

There are already some lessons that can be learnt: New Zealand developers of generative AI tools need to be cautious about what data they use to train their models. That is the case even if these cases fail in America. New Zealand lacks the broad "fair use" defence to copyright infringement, so a claim in copyright infringement here might go further than it does in America.

And for those excited by the idea that there might be a ChatGPT-style AI that can produce basic advice and replace law graduates, look out for the accuracy ratings of these tools and perhaps consider how that phone call to the liability insurer might go – in the short term at least. ■

Andrew Easterbrook is a director at Webb Ross McNab Kilpatrick Lawyers (WRMK Lawyers) ■

unethical manner to cheat, plagiarise or misuse it in some other manner.

There are varying views about the experience AI can deliver to students, in particular. It can be used to personalise their learning experience and offer real-time feedback to both students and teachers. ChatGPT, in particular, can also help with grading, generate reports and deal with frequently asked questions, freeing up time for educators to focus on more creative and engaging teaching methods.

In the absence of a standard or regulation around the use of AI, and more specifically chatbots, educational facilities such as New Zealand's eight universities are attempting to align their individual AI policies.

Some aspects for consideration of ethical AI practices can include:

- Program and algorithm developers questioning the consequences of the design at development stage;
- Regular and thorough audits to be conducted on the data collected from a new AI product, along with seeking responses from developers, society and others impacted by the product to detect and possibly deter bias; and
- Instead of creating additional legislation, enable regulatory sandboxes to be created to allow for innovation both in technology and regulation. ■

Vaheeni Naidoo is an executive working with ADLS' committees ■

New Zealand lacks the broad "fair use" defence to copyright infringement

With the lack of general regulation about AI, privacy cases are dealt with in an individual manner based on country-specific regulation