



AI and the law

2023

The
Law
Association

AI and the law

Policy / Reform: A White Paper

Published by the Technology and Law Committee
of The Law Association

2023

With contributions from Alex Summerlee, Steven Moe, Amy Kingston–Turner,
Lloyd Gallagher, Vaheeni Naidoo, and Diana Clement

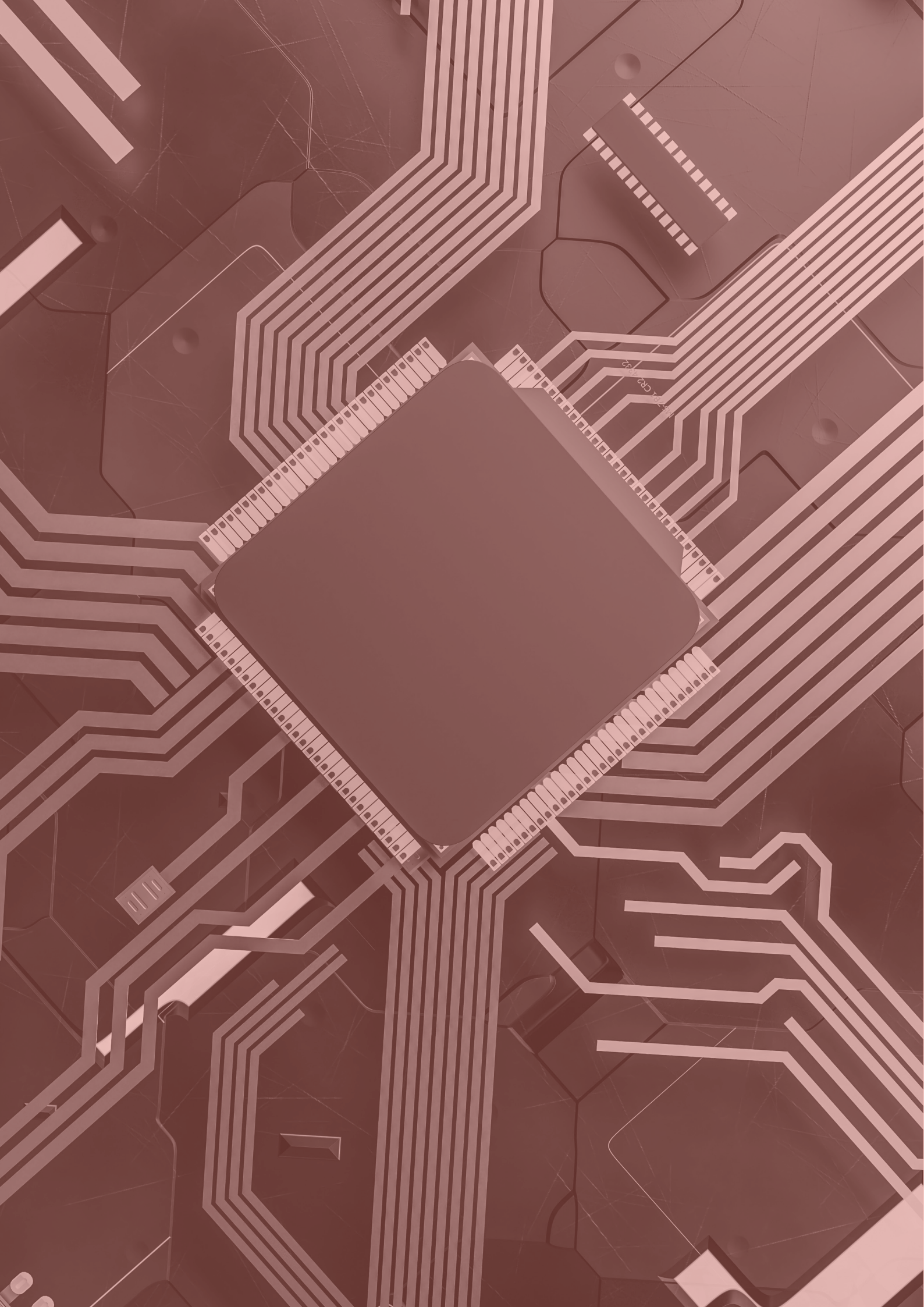
Edited by Steven Moe

CAUTION TO READER: No responsibility or liability is accepted by the Law Association Inc for the accuracy of any statement, opinion or advice contained in this publication. The views and opinions expressed in this publication are those of the individual authors, and not necessarily those of the The Law Association Inc.

While all reasonable care has been taken by the authors and the Law Association Inc in presenting this publication, the contents are intended to provide general information in summary form only, and do not constitute legal or financial advice and should not be relied on as such. Readers should rely upon their own enquiries or research before making any decisions or taking any action based upon information contained in this publication. Specialist advice should be sought in particular matters.

Contents

- 7 Introduction
- 9 AI and Copyright: Battle lines drawn for a stoush between ChatGPT and copyright law
by Steven Moe and Alex Summerlee
- 11 Privacy and AI: Safeguarding rights in the age of artificial intelligence
by Amy Kingston-Turner
- 15 Harnessing AI tools in legal businesses: Advancements, risks, and data handling
by Lloyd Gallagher
- 22 Ethical considerations of artificial intelligence
by Vaheeni Naidoo
- 25 Advertisers beware: click fraud is on the rise
by Lloyd Gallagher
- 27 Navigating the legal complexities in remote virtual inspections
by Lloyd Gallagher
- 31 Leveraging AI technology in real estate: advancements, risks and data management
by Lloyd Gallagher
- 35 How generative AI will impact the way lawyers work
by Diana Clement



Introduction

Artificial intelligence has been around for a long time but has until recently seemed like something for a sci fi movie rather than a technology with practical impact. That changed at the end of 2022 when AI burst onto the scene with the buzz around ChatGPT. Since then, the level of media attention and focus on the potential of artificial intelligence has been enormous as this new tool and its impact is better understood.

There will certainly be an impact on the role of lawyers as a result of this new technology. But will it be similar to past technologies such as telex, fax, Blackberry, typewriter, computers and the internet, all of which aided lawyers' work? Or does AI represent a more fundamental shift in the nature of the work we do?

In this white paper we want to be proactive in imagining the future and, by doing so, anticipate and highlight issues we think need consideration from a policy perspective. Some points we make might signal areas where legal reform is also needed.

At the end of each topic, we have included three pertinent policy questions to provoke discussion. We hope this paper will be useful to those in government, Members of Parliament, councils, those drafting regulations and laws and those who are curious about where we are headed.

This is the first in what we hope will become a series of white papers produced by The Law Association. We hope it is challenging, makes you think and encourages regulators to consider the issues that arise from new technology.

Steven Moe

Editor and member

The Law Association's Technology and Law Committee

stevenmoe@parryfield.com



AI and copyright

Battle lines drawn for a stoush between ChatGPT and copyright law

by Steven Moe and Alex Summerlee

[This was first published by ADLS on 9 June 2023](#)

A legal brawl is brewing about how, and whether, copyright law should apply to the use of artificial intelligence chatbot, ChatGPT. In one corner are authors who own copyright in their work; in the other are those who claim there is a public interest benefit in enabling content (or 'output') from AI such as ChatGPT to be exempt from copyright restrictions.

ChatGPT operates by harvesting the work of others to produce content for its users. The problem is that this output may breach the copyright of the original author.

ChatGPT's process works like this: the chatbot's machine learning algorithm mines vast datasets, including texts, websites, news articles and books to respond to users' prompts. This process uses billions of parameters to statistically analyse complex language structures and patterns, from which it can produce sophisticated and surprisingly accurate content.

Authorship

To unpick this issue, it first needs to be asked who authors the text generated by ChatGPT? The person who put in the prompt? Or is it OpenAI, the company that released ChatGPT onto the market in November 2022?

Under the Copyright Act 1994, the author of a computer-generated work is "the person by whom the arrangements necessary for the creation of the work are undertaken". Arguably, as the person inputting the prompts into ChatGPT, the user becomes an author of the output created by

the AI.

OpenAI might also be a joint author. It has taken a stand on this and, perhaps surprisingly, its terms of use provide that OpenAI assigns all title and interest in the output to the user. This suggests OpenAI considers it might have some claim to authorship but it is quick to divest itself of any title to that output. And while output from ChatGPT might be authored by the user, that work may not itself attract copyright. For this to happen, the work must be original and to be 'original' the author must have exerted a sufficient degree of skill or labour in producing it.

Can it be said that the person inputting a prompt into ChatGPT exerted any skill or labour in producing the output? It is an arguable point: some consultants are forging new careers in creating the best prompts. Even if this is so, will some output end up being so similar to the work of others that it becomes a copy of another's work? Chances are that your average AI user has not reflected on whether his or her use of ChatGPT might infringe copyright. It is likely that many users intuitively think the AI is the author of any output. However, rightly or wrongly, the narrow description of who (and

what) can be an author for the purposes of the Copyright Act probably means the AI itself is not the author.

The risks

The million-dollar question is whether there is a risk that a ChatGPT user might inadvertently infringe on someone else's copyright work. For example, this could occur where the output reproduces a portion of copyright-protected material. This raises several policy questions. Does the author of a copyright work have a legitimate interest in that work being protected from a ChatGPT user's inadvertent infringement into that copyright? Is there a public interest in the benefits of AI for such output to be an exception to the infringement regime in the Copyright Act?

The Copyright Act provides for some exceptions, including, for example, the fair dealing exception. This means copyright in a work is not infringed "if such fair dealing is accompanied by a sufficient acknowledgement". The trouble is that output does not provide (at least for now) any acknowledgement of what work

[Continued on the next page](#)

has been trawled from the internet to produce its output. What are ChatGPT users to do with this? Do they run the gauntlet and hope their output does not infringe on someone else's copyright work?

Overseas solutions

Some work on this issue has already been done in the UK and in the European Union. Their laws have been updated to offer guidance around how copyright protections work in respect of AI-produced output.

They provide two models for AI exceptions, allowing what otherwise would be a copyright infringement, and give some idea of what reform of the Copyright Act, in respect of AI, could look like in New Zealand. The EU has two copyright exceptions for text and data mining which specifically permit the use of data to train LLMs (the large language models that power ChatGPT). Broadly speaking, these exceptions provide for:

- Text and data mining for the purposes of scientific research, innovation and education. This enables "non-commercial" research organisations and cultural heritage institutions to data mine (eg, universities, museums, etc.); and
- A general exception from copyright infringement for anyone, including commercial enterprises, using text and data mining.

However, a rights-holder can contract out of this latter exception, meaning that the copyright holder can reserve the rights to carry out text and data mining of their work, and thereby prevent others from doing so. The UK has taken a more narrow approach – so far. Its Copyright Designs and Patents Act 1988

provides a limited exception to copyright infringement, similar to the first category of EU exceptions.

The exception provides that text and data mining does not infringe copyright where it is done for the purpose of computational analysis for non-commercial research. Further, for the exception to apply, sufficient acknowledgement of the mined work must be given.

Some commentators have noted that these restrictive approaches do not allow for the full potential benefits of AI to be exploited. That's why the UK government confirmed its intention to expand the scope of that exception to enable text and data mining of works protected by copyright and database rights for any purpose because of the benefits to artificial intelligence and wider innovation in the UK. However, the minister responsible for the policy faces strong opposition to the proposal. While this article has focussed on the text generated by AI, another open question relates to images created using prompts. Should that be considered more as "art" with different protection?

Where to next?

There are myriad problems coming our way, along with new policy issues around the legitimate interests of authors who create content mined by AI versus societal interest in the advantages that AI data mining can contribute to the common good.

We'll leave it for readers to weigh up how that tension should be settled. And if all else fails, we can always ask ChatGPT how it should be solved.

Steven Moe and Alex Summerlee are partners at Parry Field Lawyers in Christchurch

Policy questions

- Is copyright law in need of reform in this area?
- Who should own content produced by AI?
- How should we recognise the original sources of ideas that large language models utilise?



Privacy and AI

Safeguarding rights in the age of artificial intelligence

by Amy Kingston-Turner

As the chatter about AI's role in our society becomes louder, the inherent connection between the ethical, legal, and practical aspects of existing privacy laws and forthcoming AI regulation becomes clearer. This article explores the relationship between privacy laws and AI regulation, highlighting the existing ethical frameworks we can work within, the practical challenges we face, and the need for a collective effort to shape the future of technology while safeguarding privacy and ethical values.

In the age of artificial intelligence, our lives have become increasingly intertwined with technology, granting us unprecedented convenience and efficiency. However, this technological leap forward has also created a host of privacy concerns. At the heart of these concerns lies a delicate balancing act, as the power of AI often clashes with the right to privacy, a right which is fundamental to many modern societies and is enshrined in the Universal Declaration of Human Rights.

Existing privacy issues in AI systems, including a lack of transparency, the failure to minimise data collection and retention, the challenge of obtaining meaningful consent and the

inability to effectively delete personal information have been well documented.

Regulations targeting AI have been in the works in multiple jurisdictions since before the advent of ChatGPT, which propelled AI into the imaginations of the masses.

When looking at these developing regulations, it becomes clear that there are intersections with already established privacy regulatory frameworks. Key themes central to the regulation of personal information, such as transparency, fairness, security and accountability are mirrored in the ongoing discussion surrounding AI governance. Ethical considerations around algorithmic transparency,

accountability, bias and the need for human oversight have emerged as key themes in most existing and emerging AI governance frameworks and regulatory proposals. In essence, an ethical approach that is already well established in the world of privacy regulations is also becoming central to AI governance discussions.

In fact, many of the existing privacy regulations can, and do, already apply to the regulation of AI tools to the extent that they are processing personal information. These laws carry provisions that demand algorithmic accountability and fairness – for example, requirements around consent and transparency, although

Continued on the next page



the extent to which AI models can currently comply with these provisions remains unclear, and is a topic for another discussion.

Indeed, good data governance, including its source, quality and ethical usage is key to complying with existing privacy laws, and is emerging as vital to AI governance. It is evident that the regulations safeguarding our personal information can act as building blocks for the ethical and legal considerations surrounding regulation and management of artificial intelligence.

In this ever-evolving landscape of technology and data, organisations find themselves at a juncture where the lessons learned from establishing now-mature privacy programs can be effectively extended to navigate the emerging and immature governance of artificial intelligence.

Having weathered the introduction of global privacy laws, businesses have amassed a wealth of experience and expertise that can be channelled and adapted into the realm of AI governance. In the same way that meticulous scrutiny of data is inherent in compliance with privacy regulations, the necessity for a solid understanding of data and data flows is now also critical to AI considerations. For example, organisations can integrate questions concerning the use of AI into their existing Privacy Impact Assessments, enabling them to identify and mitigate high-risk AI applications through ethical human intervention. This convergence of privacy and AI governance in practice underscores the pivotal role that established privacy programs can play in developing responsible AI management practices.

One area where regulators may choose to distinguish the developing AI regulations from existing privacy regulations is in the area of remedies available for a data breach.

Large language models, such as ChatGPT are fed colossal datasets that encompass depersonalised and personal data. The tech giants of our time, including Apple, Alphabet and Meta, have mastered the art of profiting from data collection by extracting and utilising data for various purposes. It is notable that, to date, remedies for data breaches have primarily been evaluated in terms of the harm inflicted on individuals rather than considering the substantial profits amassed by the companies responsible. A paradigm shift that focuses on profits made rather than harm caused when evaluating liability may be essential in fostering a more comprehensive and equitable approach to data privacy in the age of AI.

While existing ethical principles provide a solid foundation for mitigating the risks associated with AI, the real-world application of these principles is complex and evolving. What is considered ethical behaviour can be subjective and differs across the globe. Therefore, in order to address some of the issues that AI raises, everyone, including developers, policymakers, businesses, and ordinary citizens must familiarise themselves with AI's inner workings to make informed decisions about AI's associated risks and benefits. For businesses navigating this area, a risk-based approach, tailored to each business and AI tool, becomes imperative. To do this, businesses must intimately understand their

own risk appetite, a factor that will influence their choices regarding AI utilisation. Ongoing risk assessments, akin to those in the privacy domain, will become important to manage unforeseen consequences arising from use of AI. Human oversight remains the primary check and balance. Additionally, effective lifecycle management must be in place to address the continuous evolution and improvement of AI systems.

The rapid ascent of AI may forever alter the way we live and work, and the fusion of privacy laws and AI governance is a solid foundation on which we can build. While established principles around the governance of personal information provide a solid framework for ethical AI, the practical application of these principles requires collective effort and a deep understanding of AI's inner workings and potential risks.

In essence, the evolving landscape of AI governance requires us all — developers, policymakers, lawyers, and citizens — to maintain a commitment to human oversight and continuous education. It is only through such efforts that we can strike the delicate balance between technological advancement and the preservation of fundamental human rights in an increasingly interconnected and AI-driven world.

Amy Kingston-Turner is a director of Source New Zealand, as operated by Hamilton Locke (NZ) Limited

Policy questions

- Does AI require its own regulation in New Zealand?
- Do existing ethical frameworks already inherent in global privacy regulation provide a solid foundation on which to build AI regulations?
- How should data breaches in the age of AI be remedied?
- How can businesses start to manage their own AI risks now, in the absence of current regulations?



Harnessing AI tools in legal businesses

Advancements, risks and data handling

by Lloyd Gallagher

Artificial Intelligence (AI) is transforming much of how we do business and the legal industry is no exception. Integrating AI tools into various aspects of legal practice is becoming standard and a surge of new technology has developed, aimed at increasing efficiency.

These advanced technologies offer immense potential to streamline operations, optimise research processes and deliver valuable insights for legal professionals. However, along with these benefits it is crucial to address the potential risks associated with AI tools and their implementation, especially concerning data privacy and security.

Here we will explore the AI tools commonly used in legal businesses, delve into the importance of data handling and highlight the risks and measures to mitigate them.

Part I: AI tools for legal businesses

Document review and analysis
AI-powered tools like contract analysis platforms and eDiscovery solutions are widely used in legal businesses for document review and analysis. These tools utilise natural language processing (NLP) algorithms to extract relevant information, identify key clauses and categorise documents efficiently. Microsoft, IBM, Relativity, Kira Systems and ROSS Intelligence all provide solutions in document analysis to deliver due diligence and analysis to assist with efficiency.

Legal research

AI-driven legal research tools have transformed the way legal professionals find case law,

statutes and regulatory information. Platforms such as Westlaw Edge, LexisNexis and Casetext leverage AI algorithms to deliver precise and relevant search results.

Predictive analytics

Litigation analytics tools enable legal businesses to make informed decisions by predicting case outcomes and trends. These tools analyse historical data to provide valuable insights on judges' tendencies, opposing counsel strategies and case success rates. Lex Machina and Premonition are leading examples.

Contract management

AI-powered contract lifecycle management tools simplify the contract management process, automating tasks like contract creation, review and renewal. No-table platforms include Ironclad, Agiloft and ContractZen.

Virtual legal assistants

AI-driven virtual assistants such as Della and Eva help legal professionals with administrative tasks, appointment scheduling and basic client inquiries.

The advantages of AI tools in legal businesses

Enhanced efficiency: AI-powered tools, like document review platforms and virtual legal assistants, expedite mundane tasks, freeing up valuable time for

legal professionals to focus on more complex and strategic matters.

Informed decision-making:

Predictive analytics and legal research platforms provide data-driven insights, empowering legal practitioners to make well-informed decisions, optimise litigation strategies and assess case outcomes with greater accuracy.

Improved client service: AI-driven contract management and research tools enable legal businesses to respond promptly to clients' needs, enhancing overall client satisfaction and fostering stronger relationships.

Cost-effectiveness: Automation through AI can lead to reduced operational costs, benefiting both legal businesses and their clients by potentially lowering legal fees.

The benefit of using AI tools is clear. They provide invaluable resources to cut down human hours and offer insights quickly and efficiently. Insights that may be overlooked and data analysis that would usually require a team trawling through large volumes of information at great expense are easily handled by AI and the time saved using machine-based systems assists with access to justice.

Continued on the next page

However, AI tools are not without their pitfalls. While an AI system can deal with large volumes, it has limitations. For example, AI generated documents or articles are junior in approach. The final form is similar to that of an American undergraduate or legal executive, which is below the quality many practitioners would expect.

Currently, AI is trained around an American model of knowledge, meaning the academic approach from the United States is the approach that AI is learning, leaving a series of systems that is designed around an undergraduate approach from an American perspective in the resulting articles, documents, and analysis that are being written by AI. This results in an end-of-use product

and efficiency in creating a draft.

Just like speech to text, the information being placed on the paper is only as good as the information it is drawn from or the speech recognition being used. AI is a tool and should never be considered as a replacement for the human approach.

Now that we understand how AI

until the opposition requested the production of the authority that the information came unstuck.

Several questionable issues have arisen with the use of AI in similar industries. Results that have been put forward as legitimate have led industries and lawyers to consider what they need to be aware of when using AI tools.

Data privacy and security

One of the primary risks associated with AI tools in legal businesses is the handling of sensitive client data. Data breaches or unauthorised access to legal documents can lead to severe legal consequences and tarnish the firm's reputation.

- AI tools employed for document review and analysis often require access to large volumes of sensitive legal data. To address data privacy concerns, legal businesses must ensure data encryption during storage and transmission, implement role-based access controls and conduct regular audits to monitor data usage.
- Legal research platforms handle vast amounts of legal data. To protect client confidentiality, these tools must employ robust security measures, including secure data centres, encryption and compliance with industry standards such as General Data Protection Regulation (GDPR) for international data transfers.
- Predictive analytics tools depend on historical case data, making data anonymisation crucial

to protect client identities. Additionally, maintaining data accuracy and updating the AI models regularly are essential to ensure accurate predictions and mitigate biases.

- Contract management tools process sensitive contract data, including proprietary terms and conditions. Implementing strong access controls, data encryption, and multi-factor authentication (MFA), is essential to safeguard data from unauthorised access.
- Virtual assistants require access to personal information and calendars. Legal businesses must ensure secure data transmission and enforce strict data-retention policies to protect client privacy.
- All the data listed above is sensitive in nature as it provides information on where people will be located, information on cases that may hold sensitive data and information that is often privileged and not wanted in any other media but a secure server. This has given rise to questions about the way data is handled by the provider, where it is stored and how it is accessed, shared or used for training AI, which are questions yet-to-be answered by many firms but have prompted privacy policies.

The result from ChatGPT is clear: open AI has a policy that prevents use of information and retention beyond the current conversation. However, even AI appears unaware of how data is used in its own training. While it confirms it strips personal data, it is unclear what is considered personal.

Personal information can often relate to data that could be used to identify another – this information is not considered personal under the policies and still gives rise to questions about the way data is being stored and retained and how it is used in its training, which is a big issue for law firms and cannot be taken lightly. Accordingly, while AI tools provide great benefit for law firms, care must be taken as to how they are used and what information is provided to the AI engine or bot.

Other considerations are also required when implementing any form of AI in your business. These include the quality of results from AI, as many results show there is a level of bias, issues of accuracy and liability risks as well as ethical concerns. Below we will explore some of these concerns.

Bias and fairness: AI algorithms may perpetuate biases present in the data used to train them, as well as historical results that AI has obtained. Many biases still exist within the legal environment, based on statistical data and old judgments that remain in authority, which may lead to unfair outcomes and decisions. Legal businesses must actively monitor and address biases to ensure fair and just practices.

Accuracy and liability
AI tools are not error-proof, and relying solely on AI-generated information without proper

Continued on the next page

Therefore, while AI can provide a number of efficiencies to quickly get information before a senior, the information still needs to be reviewed, edited, cleaned, and checked for accuracy before the final product is released.

The quality, risks, and limitations of AI

When AI is asked a question, it accesses a pool of resources to formulate the result. This pool is limited in a number of ways:

- the pool of resources is based on the training data limitations
- a lack of understanding as to what is typed
- a narrow focus during the training (ie, the questions were not broad enough or the answers were not clear enough)
- ambiguity and context challenges
- creative and critical thinking limitations
- an inability to learn from experience.

These limitations mean the person training the AI must have a great understanding of how people and computers will engage with the information being input. If there is a lack of knowledge in this area or if the information is not clear enough for the resulting queries within the systems that AI uses, the result will be poor and clumsy.

that would be considered to be junior or from an early entrant into the legal industry. Therefore, while AI can provide a number of efficiencies to quickly get information before a senior, the information still needs to be reviewed, edited, cleaned, and checked for accuracy before the final product is released.

In many ways, AI must be considered on the same basis of any tool: it is just that, a tool. While it can provide a number of benefits, efficiencies and speed to any process within a law firm, it is unlikely it will ever be able to replace the senior lawyer with experience and knowledge of the law.

There are many reasons for this:

- the law is ever-evolving,
- twists and turns happen in case
- judgments do not always follow a standard set of human inquiry
- training AI will always lag behind the evolution of society.

That said, simple-form contract and efficiencies can be created using AI tools because of AI's speed

operates, the efficiencies it can provide and its quality limitations, we can look at the risks this poses for law firms.

Part II: Risks of using AI tools in legal businesses

Recently, a lawyer in the United States used ChatGPT to run his legal research which was submitted to the court. The lawyer claimed he was unaware that the information AI could obtain could be false. He assumed the result from AI was legitimate and true and that he did not need to take any other due diligence to confirm what was being written.

The argument failed because ChatGPT has a fall-back position where AI stipulates that the information could be incorrect or inaccurate. However, the lawyer continued to rely on the result and submitted it to the court as accurate with an AI argument that was very compelling. It was not



verification can lead to incorrect advice and potential legal liability. Ethical concerns: AI's application in legal matters raises ethical questions, especially when it comes to the use of AI in critical decisions concerning human rights, civil liberties and sensitive personal matters.

Over-reliance on AI: While AI tools enhance efficiency, legal professionals should not entirely rely on them. Human expertise and judgment remain crucial in complex legal matters, requiring a balanced approach.

Expanding on the risks: how do we mitigate?

Data breaches

AI tools often rely on large datasets to learn and improve their performance. This data might include confidential client information, financial records, medical history and other personal details. A data breach where this sensitive data is exposed or stolen can lead to severe repercussions, such as identity theft, financial fraud and damage to the client's reputation.

Mitigation: Legal businesses must implement robust data encryption, employ secure data-storage practices and regularly update security protocols. Additionally, having a well-defined incident response plan can help in promptly addressing and containing data breaches if they occur.

Inadequate data anonymisation

AI algorithms used in legal businesses often rely on historical case data, which might include identifiable information about clients and parties involved. Improper anonymisation of data can lead to unintended identification, violating client privacy and confidentiality.

Mitigation: Legal businesses should ensure AI training data is thoroughly anonymised before being

used in AI models. Techniques like differential privacy can help protect individual identities while maintaining data accuracy for AI learning.

Cross-platform data sharing

AI tools may require data integration from multiple sources, which could lead to cross-platform data sharing. When data from different systems is combined, the risk of privacy breaches increases, especially if proper consent is not obtained from the individuals concerned.

Mitigation: Legal businesses must have clear data-sharing agreements with third-party AI tool providers, ensuring data is shared only for specific and legitimate purposes. Additionally, explicit consent should be obtained from clients before sharing their data with AI tool vendors.

Profiling and surveillance

Some AI tools, particularly in predictive analytics, might inadvertently lead to profiling and surveillance concerns. AI algorithms may

analyse client data and behaviours, potentially identifying patterns and characteristics that could be misused or lead to discriminatory practices.

Mitigation: Legal businesses must conduct thorough impact assessments before deploying AI tools. It is essential to regularly audit AI models for bias and discriminatory outcomes and implement necessary corrections to ensure fairness and compliance with data-protection regulations.

Lack of transparency

AI algorithms often work as "black boxes", making it challenging to understand how they arrive at specific conclusions or decisions. This lack of transparency can raise concerns about the handling of client data and decision-making processes.

Mitigation: Legal businesses should strive to use AI tools that provide interpretable results and maintain transparency with clients about the use of AI in their cases. Educating clients about the benefits and

limitations of AI can foster trust and mitigate privacy concerns.

The adoption of AI tools in legal businesses not only presents privacy and ethical concerns but also introduces legal risks that must be carefully navigated. These risks can have serious implications for legal practitioners and their clients, potentially leading to legal challenges and liabilities. Let's explore the legal risks associated with AI in legal businesses:

Malpractice and professional responsibility

When legal professionals rely heavily on AI tools for critical decision-making, there is a risk of misconduct if errors or inaccuracies occur. Lawyers have a duty to exercise reasonable skill and care in handling their clients' cases. If AI tools lead to negligent advice or inappropriate legal actions, the legal business could face misconduct claims and reputational damage. Mitigation: Legal practitioners should exercise caution when using AI tools and verify their results before making decisions. They

must also maintain communication with clients, ensuring AI-generated advice is appropriately explained and supplemented with human expertise.

Compliance with legal standards AI tools must comply with various legal standards, including data-protection laws, intellectual property rights and industry-specific regulations. Failure to adhere to these legal requirements can lead to legal actions, fines and sanctions.

Mitigation: Legal businesses should conduct thorough due diligence before adopting AI tools. Ensuring the tools comply with relevant laws and regulations can help mitigate potential legal risks.

Intellectual property infringement Some AI tools might be developed using proprietary algorithms or datasets. If legal businesses use such tools without proper authorisation or licensing agreements, they could be at risk of infringing intellectual property rights, leading to legal disputes and

financial penalties.

Mitigation: Legal businesses should carefully review the terms of use and licensing agreements associated with AI tools. Seeking legal advice when unsure about the intellectual property rights of AI vendors can help avoid infringement issues.

Lack of legal oversight

As AI tools become more sophisticated, there might be a lack of legal oversight and clear regulations governing their use. This ambiguity can lead to uncertainty and potential legal challenges about the validity and admissibility of AI-generated evidence in court.

Mitigation: Legal practitioners should stay informed about the legal landscape surrounding AI tools and their application in the legal field. Engaging in professional discussions and seeking guidance from legal associations can contribute to shaping clearer legal guidelines.

Bias and discrimination in AI algorithms

AI algorithms might inadvertently perpetuate biases present in the data used for training, leading to discriminatory outcomes. If these biases result in unequal treatment or unfair practices, legal businesses could face discrimination claims.

Mitigation: Legal businesses should proactively audit AI algorithms for bias and implement corrective measures. Employing diverse and inclusive datasets during AI training can also help reduce the risk of biased outcomes.

In this next section, we will look at how AI can be cautiously embraced to enhance your legal business. Navigating AI in legal businesses As discussed above, AI is not without its risks and problems. Integrating AI tools into legal businesses has undeniably transformed the legal landscape, offering numerous advantages such as streamlined processes,

Continued on the next page

improved research capabilities and data-driven insights.

However, the benefits of AI must be approached with caution, as AI introduces inherent risks that demand thoughtful consideration and responsible implementation. In this section, we explore the potential benefits and risks of using AI in legal businesses and argue that a cautious approach is essential to ensure ethical, legal and privacy standards are upheld.

To summarise, the risks of AI in legal businesses are:

Data privacy and security: AI tools often require access to vast amounts of sensitive client data, raising concerns about potential data breaches and unauthorised access.

Bias and fairness: AI algorithms can perpetuate biases present in historical data, leading to unfair outcomes and discriminatory practices in legal decisions.

Legal compliance: The complex legal landscape surrounding AI necessitates careful adherence to data-protection laws, intellectual property rights and other regulations to avoid legal liability and penalties.

Ethical considerations: Employing AI in sensitive legal matters may raise ethical dilemmas about the role of technology in making critical decisions that impact human rights

and civil liberties.

The path forward

While embracing AI tools can undoubtedly bolster legal businesses' efficiency and effectiveness, a cautious approach is crucial to mitigate potential risks and ensure ethical practices. Legal practitioners should:

- prioritise data privacy. Implement robust data encryption, access controls and regular audits to safeguard client information and prevent data breaches.
- address bias and transparency. Proactively audit AI algorithms for bias, strive for algorithmic transparency and use diverse and inclusive datasets to promote fair and unbiased outcomes.
- stay informed and compliant. Keep abreast of evolving legal regulations and ensure AI tools comply with relevant laws and industry standards.
- supplement AI with human expertise. Recognise that while AI tools are powerful aids, they should complement rather than replace human legal expertise and judgement.

The legal industry can only benefit from AI tools which have brought transformative advancements to the profession, improving efficiency, accuracy and client service.

However, the risks associated with AI, including data privacy, bias, legal compliance and ethical

considerations must not be underestimated. A cautious approach to AI implementation, coupled with proactive measures to address potential risks, will enable legal businesses to harness the benefits of AI responsibly while safeguarding client privacy, upholding ethical standards and maintaining compliance with legal regulations.

Ultimately, a thoughtful and cautious embrace of AI will ensure the legal industry continues to evolve in a manner that serves the best interests of both legal practitioners and their clients.

Conclusion

AI tools offer remarkable advantages for legal businesses, ranging from streamlined document management to data-driven insights. However, the risks of breach of data privacy and security, biases, over-reliance, inaccuracy and ethical concerns must be acknowledged and addressed diligently.

By implementing robust data-handling practices, regularly auditing AI models for biases, and maintaining a balance between human expertise and AI assistance legal businesses can harness the potential of AI responsibly, ensuring the best outcomes for their clients while upholding ethical and legal standards.



Ethical considerations of artificial intelligence

by Vaheeni Naidoo

Artificial intelligence (AI) plays a significant role in our lives. It has vastly improved the manner and capability with which we do things.

Research shows more than 50% of companies globally, especially in emerging nations, have adopted AI for at least one function. It is used in all sectors, from optimising service operations through to recruitment, the capture of biometric data, judicial systems and finance. So, AI is ultimately making key decisions in people's lives.

Although it brings multiple advantages, the use of such technology poses both risks and challenges. It is therefore imperative to consider the ethical implications posed by the use of AI.

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, AI emanates

from programs and algorithms which are generated by humans. These programs analyse, disseminate and study information effectively, while 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 stems from the fact that it is crafted by ultimate human programming.

Discrimination and bias

Artificial intelligence bias is regarded as the underlying prejudice upon which AI is created. It can lead to discrimination and have other social impacts which raises heightened ethical concerns. In such instances, both human bias and any resulting discrimination can be replicated when programs or algorithms are developed.

According to The 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 housing opportunities and so forth. In some instances, the output of AI can be regarded as replicating bias.

Since 2019, the Dutch government has been involved in a scandal about a self-learning algorithm used by the tax authorities to detect fraud in respect of those applying for childcare benefits. In such instances, families were penalised on a mere suspicion of fraud, based on an algorithm, and thousands of families were led to poverty. Sadly, some committed suicide whilst several children were incorrectly placed in foster care.

Privacy

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

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

The ultimate question remains as to whether an individual would even be aware that his or her data was even collected, which might have allowed them to make a reasonably informed decision as to next steps about the retention of their data.

It is important to note that even when data is publicly available, its use 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. 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, 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 (OAIC) 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 the OAIC and the UK's ICO confirming an 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

As with most technology, the challenge is not the technology itself, but rather our human emotions, experience, and reaction to it.

— Alex Sims

Professor, University of Auckland Business School

and delete the data.

Plagiarism and related effects

Recently, plagiarism concerns about ChatGPT have been widely published by 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, compose articles and provide responses to questions.

Accordingly, concerns about ChatGPT relate to whether the information obtained will be used in an unethical manner to cheat, plagiarise or misuse information.

There are varying views about the experience AI can give students, in particular. It can be used to personalise the learning experience for students and to offer real-time feedback to students and teachers. ChatGPT, in particular, can also help with grading, generating reports and answering 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 about the use of AI, and more specifically chatbots, in education, New Zealand's eight universities are attempting to align their individual AI policies.

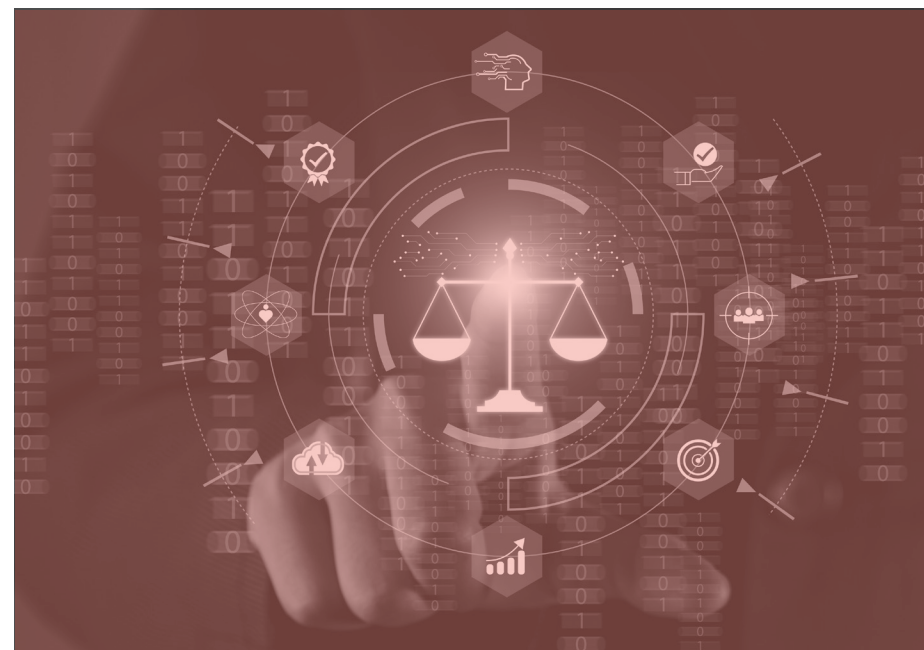
There are no global laws overseeing AI and its development and usage, which leaves the ethical aspects of AI usage unclear.

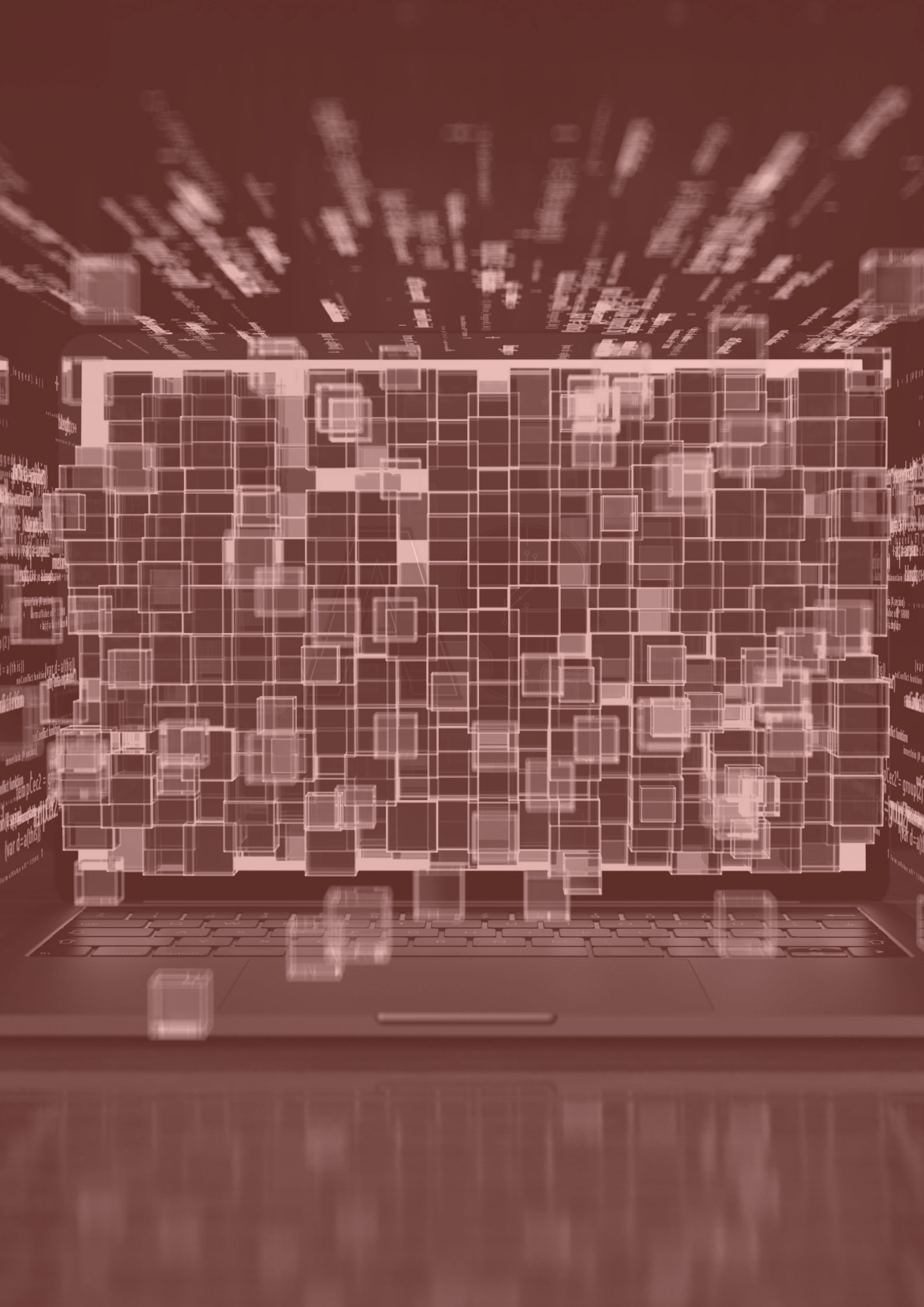
Globally, there are discussions about the under- and over-regulation of AI, both of which pose ethical concerns. While there are several legal guidance aspects around consent and appropriately informing users, the legal interpretation and practical implementation of requirements such as AI fairness is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

As Professor Alex Sims from the University of Auckland Business School says in her article *ChatGPT and the future of university assessment*, "As with most technology, the challenge is not the technology itself but rather our human emotions, experience and reaction to it."

Policy questions

- For program and algorithm developers to question the consequences of the design at its development stage.
- For regular and thorough audits to be conducted on the data collected from a new AI product and to receive responses from developers, society, and others impacted by the product to detect and possibly deter bias.
- Instead of creating additional legislation, allow for regulatory sandboxes to allow for innovation, both in technology and regulation.





Advertisers beware

Click fraud is on the rise

by Lloyd Gallagher

Impression-farming has long plagued programmatic advertising. Platforms like Google Ads and Facebook Ads use the technique to generate a range of products and services to increase advertisers' reach. Essentially, advertisers pay for targeted visits to their website, landing page or app, regardless of any purchase or engagement.

When PPC (pay-per-click) is working correctly, the fee is trivial because the click is worth more than what you pay for it. For example, if you pay \$3 for a click but the click results in a \$300 sale, then the PPC has resulted in a net gain. If the click results in nothing, then the net loss is \$3.

The most common example is search-engine marketing, as done by Google, which is also the most popular forms of PPC. It allows advertisers to bid for ad placement in a search engine's sponsored links and when someone performs a search related to their business offering, the advert will show in an appropriate rank based on the successful bid.

The industry has always been plagued with PPC fraud risk. A PPC fraud happens when someone or something clicks on your ads maliciously, without any intention of buying your product or service – for example, bots, competitors or click farms. It can waste advertisers' budgets, lower conversion rates and damage the advertisers' reputation. To prevent PPC fraud, advertisers are provided with steps to monitor campaigns and look for any suspicious patterns or spikes in traffic.

However, AI is changing the field through its ability to generate and

disseminate clicks at an alarming rate before advertisers can spot it. This paper will outline some of the issues already present and raise potential questions for providers and regulators.

How click fraud works

Large-scale click fraud is typically automated with a bot or some other program that appears to be a legitimate visitor on a webpage.

Typically, the bot clicks on an ad repeatedly with the goal of tricking a platform into thinking it is a user with the intent to purchase whatever the ad is selling. A victim of click fraud is likely to notice a large number of clicks coming from one computer and this traffic also appears suspicious to the advertising networks and advertisers.

But fraudsters can get around this by routing bot traffic through different internet protocol addresses that continu-

ally change, using a virtual private network (VPN). They can also carry out click fraud by using several computers in different geographic locations to avoid detection. However, these campaigns required a number of elements and computer connections which are easier to monitor, and options of real-person identification can be implemented, mitigating the risk.

How AI is changing the game

AI can simulate multiple affiliate connections and clicks that appear to be legitimate new traffic and clicks. Further, the speed at which AI can generate the attack is in the millions-per-second. Think of AI as having the superpower to amplify audience fraud

Continued on the next page

“
Think of AI as having the superpower to amplify audience fraud programmatically.
”

programmatically. What may have been human-staffed click or impression farms can now get boosted by smart bots to falsify impressions and attract ad dollars. AI can not only create the bad content but also fake the traffic going to the sites, at the same time creating fake accounts on advertising exchanges.

If you wanted, you could easily create AI to make hundreds of thousands of websites with bogus advertising impressions that might look like valid traffic. Advertising impression from Tik Tok, Facebook, and other media all produce an increasing risk of this exasperated approach and at a speed that is out there before it can be caught.

The result is catastrophic in the sense of fake content (bad inventory), cross-click in PPC and websites with fake engagement. In one example on Tik Tok, a creator showed how 25,000 websites could be created in minutes that then linked to advertising connections and impressions that pushed all competitors out of the Google rankings. This is only the tip of the iceberg.

This This form of fraud is estimated to have cost marketers more than US\$35 billion in 2020.

Traditional developments have produced algorithms that learn from data to perform tasks that previously required human judgment. Algorithms have historically been understood as programs that execute instructions sequentially until reaching a solution.

Artificial intelligence, in comparison, uses nonsequential approaches to reach, most often nondeterministic, one potential solution. Algorithms and artificial intelligence use data that have been restructured, formatted and prepared for process-

ing. Automated decision-making, in turn, uses algorithms or artificial intelligence to collect, process, model and use data that enable automated decisions or recommendations and, in most cases, automated decision-making systems.

This rise in AI-automated decision-making creates a substantial difficulty in determining attack vectors and legitimacy of engagement that may result in significant losses to advertisers.

Conclusion

To address the issues of AI-generated PPC fraud and bad inventory, it is important for platforms like Tik Tok, Facebook and Google to implement robust measures to detect and prevent fraudulent activities.

This may involve advanced algorithms and machine learning techniques to identify suspicious patterns, monitor website content and verify the authenticity of advertising impressions.

Additionally, regulatory bodies and industry organisations should collaborate to establish guidelines and standards for advertising practices in the context of AI. This can include stricter verification processes for website owners, transparency requirements for advertisers and penalties for those found engaging in fraudulent activities.

Overall, combating the misuse of AI in generating fake advertising impressions requires a multi-faceted approach involving technological advancements, industry regulations and cooperation among stakeholders.

Policy questions

- Should s 240(2)(c) of the Crimes Act be extended to include a definition for deception using AI?
- Should PPC providers be responsible for fraudulent attacks?
- Should AI best practices be developed for the PPC industry?

Navigating the legal complexities in remote virtual inspections

by Lloyd Gallagher

Artificial Intelligence (AI) is impacting the way strata operations can be managed. One such adaptation is the increased use of remote virtual inspections (RVIs) in various industries, including construction, manufacturing and real estate.

While these virtual inspections offer numerous benefits, such as cost savings and increased efficiency, they also raise several legal implications that businesses must consider.

The use of RVIs has surged, particularly in New Zealand and Australia, as businesses seek innovative ways to ensure continuity amidst the covid-19 pandemic. This paper delves into the multifaceted legal intricacies surrounding RVIs in these jurisdictions, emphasising the paramount importance of addressing privacy concerns, potential liabilities, jurisdiction-specific regulations, intellectual property implications, contractual nuances and steadfast compliance.

By undertaking an in-depth exploration of these aspects, this paper aims to guide managers and real estate personnel in conducting RVIs that are not only efficient, but also legally sound.

Privacy concerns: a delicate balancing act

One of the primary legal concerns surrounding RVIs is the issue of privacy. The use of video-conferencing tools and drones to conduct inspections may inadvertently capture sensitive information or images of individuals who have not consented to being recorded.

This raises potential privacy violations. Both New Zealand's Privacy Act 2020 and Australia's Privacy Act 1988 lay down comprehensive guidelines on the collection, use and disclosure of personal information. This includes data obtained during RVIs and organisations, agents and marketers must consider these principles on all data collected.

In obtaining footage, photos or video in any given area, there will always be a risk of capturing data that is not consented. Agents, managers and operators should consider the need for obtaining informed consent from individuals whose data might be captured during RVIs or providing notice in the area several months before undertaking the data collection activity.

Organisations, agents, strata managers and businesses wishing to use RVIs in any area must be diligent in acquiring this consent. They should clearly articulate the purpose of data collection and provide information on data usage and storage, with clear procedures and recording of the actions taken so it can be used to confirm diligence if a complaint is raised.

When data has been collected under the consent process, stringent data-security measures are required to maintain the data's security against breach of privacy.

The need to safeguard sensitive data from breaches is of utmost importance under New Zealand and Australian privacy principles. Given the potential legal and financial consequences of data breaches, it is in the best interests of parties to have the contracted agency confirm how the data is collected, stored and managed, and how that data is deleted or maintained. Failure to do so may result in liability, as we discuss in the next section.

Liability for inaccurate assessments: navigating the legal maze

Another legal implication of RVIs is the potential for liability arising from inaccurate or incomplete assessments.

When inspections are conducted and data is collected remotely, inspectors and agencies may face challenges in obtaining a comprehensive understanding of a site or property. Data may be extrapolated and AI may fill in sections based on assumptions from input data, which could lead to errors or omissions in reports.

These inaccuracies may result in legal disputes, particularly if the inspection or data findings are used as the basis for decision-making or contractual obligations. To minimise this risk,

Continued on the next page

managers and operators should ensure that their remote virtual inspection processes are thorough and that inspectors are adequately trained in the use of technology to conduct accurate assessments.

In the event of errors or omissions in RVI reports, inspectors may be held accountable for data considered as fallible or false, resulting in it not being able to be used. This necessitates a proactive approach that includes considerations of professional liability insurance for inspectors, as well as the way data is collected and confirmed.

Meticulous documentation of the RVI process serves a dual purpose: it bolsters transparency and can be a potent defence in case of disputes.

Jurisdiction-specific regulations: navigating the regulatory landscape

A further issue arises from local regulations. Both New Zealand and Australia, while sharing some similarities, have specific regulations governing the use of drones and other technology in RVIs. These regulations may require permits, licences or approvals, and businesses must stay informed and

compliant. Organisations should consult with legal counsel to ensure their RVI processes comply with all applicable laws and regulations.

Intellectual property issues: safeguarding knowledge and creativity

Organisations should also be aware of the potential for intellectual property (IP) issues arising from RVIs. The use of technology to capture images and data during an inspection may result in the creation of copyrightable works or the disclosure of trade secrets. To protect their IP rights, clear agreements should be established with inspectors regarding the ownership and use of any materials generated during the RVI process. Protecting trade secrets and confidential information is a paramount concern during RVIs, necessitating robust strategies to prevent inadvertent disclosures.

Contractual implications: adapting to the digital age

Organisations should also consider carefully the potential impact of RVIs on their contractual relationships. For example, a construction contract may require a physical inspection of the works by an independent third party. In

such cases, the parties may need to negotiate amendments to the contract to accommodate the use of RVIs. Additionally, businesses should ensure their contracts with inspectors clearly outline the scope of services, responsibilities and liabilities associated with RVIs.

Existing contracts may need to be revised to accommodate RVIs and any use of AI technology. This could involve renegotiating inspection clauses, redefining the scope of work and clarifying the roles and responsibilities of all parties involved. In addition, contracts with inspectors must unequivocally define the scope of RVI and AI services, including the technology employed and the expected outcomes. Clarity in contractual terms is indispensable.

Record-keeping and compliance: navigating the regulatory current

A final consideration of the general legal landscape is record retention. Both New Zealand and Australia stipulate specific record-keeping requirements. Adherence to these requirements ensures businesses can demonstrate compliance in the face of audits or legal challenges. To maintain compliance

in the evolving legal landscape, businesses must commit to regularly reviewing and updating RVI and AI procedures and documentation, aligning them with shifting laws and best practices.

How AI is being added to RVI operations

AI is being increasingly integrated into RVIs to enhance efficiency, accuracy and the overall effectiveness of the inspection process. Here's an explanation of how AI is being used with RVIs:

- **Automated data analysis:** AI algorithms can quickly and accurately analyse large volumes of data generated during RVIs. For example, in construction inspections, AI can process drone-captured images to identify structural defects, safety hazards or non-compliance with building codes. In real-time, AI can flag potential issues, allowing inspectors to focus their attention on critical areas.
- **Predictive analytics:** AI can leverage historical inspection data to predict future maintenance needs or potential risks. For instance, in manufacturing, AI can analyse machine-performance data from virtual inspections to predict equipment failures and schedule proactive maintenance, reducing downtime.
- **Image and video analysis:** AI-driven computer vision technology is used to analyse images and videos captured during RVIs. This includes identifying anomalies, measuring dimensions, detecting wear and tear or recognising defects. In real estate, AI can analyse property images to identify features like swimming pools, garages or the condition of the landscaping.
- **Natural language processing (NLP):** NLP is used to process and analyse textual data from inspection reports, emails or other documents. AI can extract key insights, flag anomalies or even generate summary reports. In the context of RVIs, NLP can

help automate the documentation process, making it easier for inspectors to communicate their findings.

- **Automation of routine tasks:** AI can automate routine inspection tasks, such as data collection and report generation. In the context of RVIs, AI-powered drones can be programmed to follow specific inspection routes and capture data automatically. This reduces the need for human intervention and minimises the risk of errors.
- **Remote monitoring and alerts:** AI-enabled systems can continuously monitor assets remotely and provide real-time alerts when anomalies are detected. This is particularly valuable in industries like energy, where AI can detect equipment malfunctions or leaks during virtual inspections.
- **Machine learning for improved accuracy:** Machine-learning algorithms can be trained with historical inspection data to improve accuracy over time. For example, in agriculture, AI can analyse drone-captured images of crops to identify diseases, pests or areas that require irrigation adjustments.
- **Augmented reality (AR) and virtual reality (VR):** AI is used in conjunction with AR and VR technologies to enhance the virtual-inspection experience. Inspectors can wear AR glasses or use VR headsets to access additional information, such as 3D models, annotations, or historical data, while conducting RVIs.
- **Autonomous inspection vehicles:** AI-driven autonomous vehicles, such as drones or robots, can perform RVIs without human intervention. These vehicles use AI algorithms for navigation,

obstacle avoidance and data collection, making them suitable for remote and hazardous environments.

- **Enhanced data management:** AI-powered platforms can efficiently manage and organise the vast amounts of data generated during RVIs. They can tag, categorise and archive data for easy retrieval, which is crucial for compliance and record-keeping.

In summary, AI is revolutionising the way RVIs are conducted across various industries. It offers the potential to streamline inspections, improve accuracy, reduce costs and enhance safety by leveraging advanced technologies like computer vision, machine learning and automation. As AI continues to evolve, its role in RVIs is likely to become even more central, providing valuable insights and driving increased efficiency in inspection processes.

Conclusion

In conclusion, the rise of RVIs presents a host of legal considerations for businesses in New Zealand and Australia. The incorporation of AI into RVI operations is also leading to increased concern of data legitimacy and privacy and includes considerations that encompass liability issues, local regulations, IP rights, contractual intricacies and compliance obligations. Consulting legal experts well-versed in the intricacies of these jurisdictions is not merely a prudent choice but an essential one, ensuring RVIs and any AI implementation is conducted efficiently, effectively and in full compliance with the law. By proactively addressing these legal complexities, businesses can harness the benefits of RVIs while mitigating legal risks.

Policy questions

- What will be the practical implications of AI for building/strata/apartment managers?
- How will it affect their accuracy, insurance and maintenance?
- What are the risks associated with using AI for firms to consider?





Leveraging AI technology in real estate

Advancements, risks and data management

by Lloyd Gallagher

Artificial intelligence (AI) is reshaping various industries and the real estate sector is no exception. AI tools have found their way into many aspects of real estate businesses, aiming to enhance efficiency and provide valuable insights. These technologies offer great potential for streamlining operations, optimising property research processes and improving decision-making for real estate professionals.

However, alongside these benefits, it is essential to address the potential risks associated with AI tools and their implementation, especially around data privacy and security. In this article, we explore the AI tools commonly used in the real estate industry, delve into the significance of data handling and highlight the risks and measures to mitigate them.

AI tools for real estate businesses

Property valuation and market analysis

AI-powered tools like automated valuation models (AVMs) and predictive analytics platforms are widely used in real estate businesses for property valuation and market analysis. These tools use data analytics and machine-learning algorithms to provide accurate property valuations, analyse market trends and forecast property prices. Companies like Zillow, Redfin and CoreLogic offer solutions in this domain.

Virtual property tours and staging

AI-driven virtual property tour and staging platforms use technologies like virtual reality (VR) and augmented reality (AR) to create immersive experiences

for potential buyers. These tools enable real estate agents to showcase properties virtually, reducing the need for physical visits and enhancing the overall buying experience. Examples include Matterport and Virtual Staging Solutions.

Lead generation and customer engagement

AI-powered chatbots and virtual assistants are increasingly used for lead generation and customer engagement in the real estate industry. These tools provide instant responses to queries, qualify leads and schedule appointments, improving the efficiency of real estate agents' communication with potential clients. Companies like Chime, Drift and BoldLeads offer AI-driven lead generation.

Automated property management

AI tools are also being employed for property management tasks. AI-driven platforms can handle tasks like rent collection, maintenance scheduling and tenant communication, making property management more efficient and cost-effective. Notable examples include AppFolio and Buildium.

The advantages of AI tools in real estate businesses

Enhanced efficiency: AI tools, such as automated property valuation models and virtual property tours, streamline processes, saving time and resources for real estate professionals and clients.

Data-driven decision-making: AI-driven predictive-analytics platforms and market-analysis tools provide data-driven insights, enabling real estate professionals to make informed decisions and develop effective strategies based on accurate market trends.

Improved customer experience: AI-driven chatbots and virtual assistants offer immediate responses and personalised interactions with potential clients, improving customer engagement and satisfaction.

Better property management: AI-powered property management platforms automate routine tasks, reducing human error and optimising property management processes.

The benefits of AI tools in the real estate industry are evident. They

Continued on the next page

offer invaluable resources to expedite processes, provide insights and enhance customer experience. However, these tools are not without their challenges and risks. Let's examine some of the key concerns and limitations associated with AI in real estate. The quality of AI in real estate While AI tools have proven their usefulness in various real estate tasks, they are not flawless and have limitations that must be considered. The quality of AI results in the real estate industry can be affected by several factors:

Data limitations: AI algorithms in real estate heavily rely on data for property valuation and market analysis. The accuracy and relevance of the data used significantly impact the quality of AI results. Incomplete and/or inaccurate data can lead to misleading valuations and predictions.

Narrow focus during training: AI models may be trained on specific geographic areas or property types, limiting their applicability to broader real estate markets. This narrow focus can result in less accurate valuations and predictions for areas or property types not well-

represented in the training data.

Bias and fairness: AI algorithms can perpetuate biases present in historical data, leading to potential discrimination or unfair outcomes in property valuations and market analysis. Biased algorithms can lead to unintended disparities in property values and market predictions, affecting both buyers and sellers.

Lack of contextual understanding: AI tools lack genuine comprehension of complex contextual factors that can influence real estate decisions, such as local economic trends, development plans or neighbourhood dynamics. Human real estate professionals often possess contextual knowledge that AI cannot fully replicate.

Over-reliance on data: While data-driven insights are valuable, relying solely on AI-generated results without considering other qualitative factors or expert judgement can lead to suboptimal decisions in real estate transactions. While AI can provide significant benefits, it is essential to acknowledge its limitations and use it as a valuable tool to complement

human expertise, rather than a replacement for human judgement.

Addressing risks in AI for real estate businesses

To harness the potential of AI responsibly and mitigate potential risks, real estate businesses must adopt certain measures:

Data privacy and security: Protecting sensitive client information is paramount. Safeguard client data from data breaches or unauthorised access by implementing robust data encryption, access controls and regular audits.

Bias detection and mitigation: Conduct regular audits of AI algorithms to identify and address biases in data and algorithms. Strive for transparency in AI decision-making processes to detect and correct biases that could lead to discriminatory outcomes.

Human oversight and expertise: Recognise that AI tools are aids, not substitutes, for human real estate professionals. Human expertise and judgment are essential for interpreting AI-generated results and making well-informed

decisions.

Continuous learning and improvement: Regularly update AI models with the latest data and market trends to ensure accuracy and relevance. Emphasise the importance of continuous learning and improvement in AI systems.

The legal risks

Under New Zealand law, the use of AI tools in the real estate industry also presents certain legal risks that need to be considered and addressed. Here are some key legal risks specific to the New Zealand legal context:

Data protection and privacy laws: New Zealand has stringent data-protection and privacy laws that govern the collection, use and storage of personal data. Real estate businesses using AI tools must ensure compliance with the Privacy Act 2020, which mandates how personal information should be handled. It is essential to obtain proper consent from individuals before using their data with AI tools and implement robust data-security measures to prevent data breaches.

Fair Trading Act 1986: The Fair

Trading Act prohibits misleading and deceptive conduct in trade. If AI tools used in real estate transactions provide inaccurate or misleading information, it could lead to legal actions under this Act. To avoid potential legal liabilities, real estate businesses should ensure that AI-generated property valuations and market analyses are accurate and not misleading.

Anti-discrimination laws: Discrimination in real estate transactions is prohibited under the Human Rights Act 1993. If AI algorithms used in property valuations or market analysis perpetuate biases that lead to discriminatory outcomes, real estate businesses could face legal consequences. It is crucial to regularly audit AI algorithms for biases and take corrective actions to ensure fair treatment of all individuals.

Contractual obligations: Real estate businesses using AI tools should carefully review their contracts and agreements with AI tool providers. Ensuring that the contracts include appropriate provisions for data handling, privacy and liability can help protect businesses from legal disputes.

Intellectual property (IP) rights: When using AI tools developed by third-party providers, real estate businesses must ensure that they have proper licensing agreements to use the tools and access the data. Failure to obtain appropriate IP rights could result in legal disputes and financial penalties.

Professional liability: Real estate professionals have a duty of care to their clients and the use of AI tools does not absolve them of this responsibility. If AI-generated information leads to negligent advice or decisions, real estate professionals could face

professional liability claims. Human oversight and expertise are essential to ensure AI-generated results are properly interpreted and used in making informed decisions.

Consumer protection laws: The Consumer Guarantees Act 1993 sets out guarantees for goods and services sold in New Zealand. If AI tools are used to provide services to consumers, real estate businesses must ensure that these services meet the required guarantees and standards.

To mitigate these legal risks, real estate businesses in New Zealand should conduct thorough due diligence before adopting AI tools, ensure compliance with data protection and privacy laws, regularly audit AI algorithms for biases and maintain human oversight in critical decision-making processes. Additionally, seeking legal advice to understand the legal implications of using AI in their operations can help real estate businesses successfully navigate potential legal pitfalls.

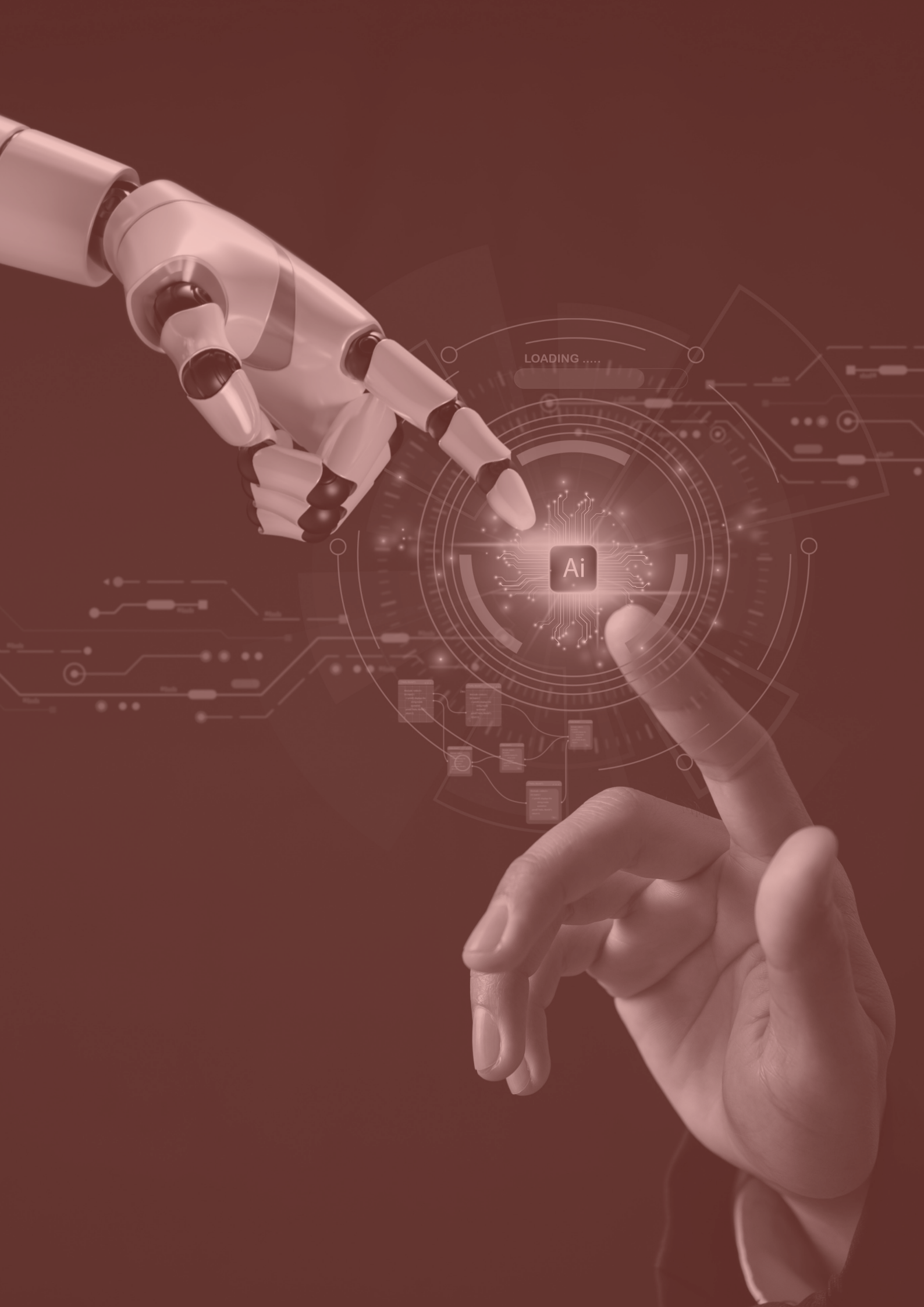
Conclusion

AI tools have become valuable assets in the real estate industry, providing efficiency, data-driven insights and enhanced customer experiences. However, to fully benefit from AI and navigate potential risks, real estate businesses must exercise caution. Addressing data privacy and security concerns, mitigating biases, recognising the limitations of AI and maintaining human oversight are crucial steps in responsibly implementing AI in real estate operations. By striking a balance between AI technology and human expertise, real estate businesses can make informed decisions, improve customer satisfaction and succeed in a rapidly evolving industry.

Policy questions

- What will be the practical implications of AI for the real estate industry?
- How will it affect its analytics, content, and legitimacy?
- What are the risks associated with using AI for firms to consider?





How generative AI will impact the way lawyers work

by Diana Clement

[This was first published by LawNews on 21 July 2023](#)

Is your graduate a cheat? As law firms begin experimenting with ChatGPT and other forms of artificial intelligence, some worry that their graduates might not have the skills their academic transcripts suggest.

Is your graduate a cheat? As law firms begin experimenting with ChatGPT and other forms of artificial intelligence, some worry that their graduates might not have the skills their academic transcripts suggest.

ChatGPT can, in seconds, generate essays and exam answers that would have taken students hours or even days in the past.

It isn't like a Google search, says Antonia Modkova, director of IP and innovation at SOUL MACHINES. "What it is generating is something novel that the world has not seen before."

The issue for both law schools and employers is that with the right prompts, ChatGPT can generate answers to complex questions. It is already good enough to pass law exams, Modkova says. GPT-4, the latest iteration of the software, scored 75% in a bar exam. "Good enough to place in the 90th percentile," she says.

For law firms wanting to hire graduates in the next few years, that could mean these students' abilities might bear no resemblance to their official academic transcript if they're skilled at using generative AI tools. Conversely, the graduates who can utilise the technology the best could prove more profitable in

private practice.

There are many uses within law firms for the technology, Modkova says. These include proofreading, legal research, drafting documents and contracts, reviewing documents and contracts, giving legal advice, automating client correspondence, summarising client meetings and even judicial decision-making.

For example, when Lawgeex used an AI robot for reviewing contracts and tested it against 20 lawyers, the robot could pick up 94% of the risks in non-disclosure agreements (NDAs). The human lawyers picked up only 85% of those risks.

Modkova adds that generative AI doesn't get bored, it writes faster than a human and is more scalable than a single legal expert charging by the billable hour.

On the downside, generative AI lacks common sense and understanding, it's extremely prone to groupthink and bias, contradicts itself and can be tricked, among other failings, she says.

Academic angst

Make no mistake, graduates will need the ability to use generative AI tools. Simply knowing the law is now not enough, says Alex Sims, associate professor in the

Department of Commercial Law at the University of Auckland Business School.

If they can't use the tools, graduates will soon be too slow in their work. The technology will only get better. But in academia, AI is generating a great deal of angst. Anti-plagiarism tools such as Turnitin are scrambling to add ChatGPT detection capability. But can these tools stay ahead of the rapidly evolving technology?

Academia doesn't yet have the answers. It's a trying time for law schools and other departments in universities everywhere, says Sims. "It means [universities] can't keep on doing what [they] did in the past." New forms of assessment are needed.

Assessing students
Law schools could focus on trying to detect AI use in written material. Or academia can try to adapt to a new paradigm, which may not be a bad thing, Sims says.

She argues that tests and exams have never been good assessment vehicles, anyway. "Just because some people are no good at exams, it doesn't mean they don't know the law."

Continued on the next page

As an example, Sims cites herself. She had no experience at sitting formal tests and exams when she entered university.

“When I was at law school, I wasn’t very good at exams because I went to a different type of school,” she says. “I would help [other students]. I’d explain what the law was to them because they didn’t understand it. And they ended up getting better marks than me in the exam because they were good at exams.”

The irony in academia, Sims says, is that universities are now considering assessment methods

Many academics are now talking about assessing soft skills which is another irony, although positive, Sims says.

“Those so-called soft skills like presenting and talking with people were dismissed [in the past].” Academics argued that law students didn’t really need the soft skills. “Now people are going ‘how can we assess students’ soft skills?’”

Why hire juniors?

It has been suggested that law firms shouldn’t worry that their graduates might have cheated in

can be automated and delegated to AI.

“However, there are key human attributes embedded in legal work which AI does not possess, including and especially critical thinking and the exercise of judgment, and the abilities to develop strategy and take account of ethical considerations.

“AI does not have the instinct, perception, or sensitivity innate in lawyers, nor does it understand or have the ability to create a trusted relationship with a client. It also does not have the practical experience a lawyer has in dealing

AI does not have the instinct, perception, or sensitivity innate in lawyers, nor does it understand or have the ability to create a trusted relationship with a client. It also does not have the practical experience a lawyer has in dealing with the unpredictable.

— **Kesia Dernhardt**
Partner, Stace Hammond

that have been superseded or ruled out in the past.

“One way that you can assess students to see whether they understand the law is in-person, handwritten assessments.” That’s assuming that good writing will still be needed in the law, as it was in the past, she says. And, of course, AI-generative tools can now do it for them, hence the need for in-person hand-written tests.

Verbal assessments could also be used to ensure students know the material. But, like hand-written assessments, these can be cumbersome and are a lot more work.

their exams because generative AI ought to be able to replace them. Why bother with self-obsessed young employees if a tool can do the job in less time?

Stace Hammond partner Kesia Denhardt disagrees. “Presently, this new technology does not have the competence to compete with lawyers so as to render them obsolete,” says Denhardt.

In fact, Denhardt argues that generative AI has significant potential to impact the way lawyers work in a positive way, by eliminating or reducing the time and effort spent on some legal work, including drafting, research, and other more routine tasks which

with the unpredictable.”

Collaboration

Denhardt argues that the optimum relationship between lawyers and generative AI would be collaboration.

“AI cannot and should not substitute for lawyers but could be utilised to work with lawyers as a tool to complement their skills and perform certain legal tasks more efficiently, thereby freeing them up to focus on the more human aspects of legal practice.”

“By joining forces, lawyers and AI could each offer one another the capability to achieve what they cannot do alone.”

Denhardt says the flow-on effects of AI being used by the profession may lead to some law practitioners changing their business model from billing on a time-spent basis to value-billing or other alternatives. It may also result in better access to justice.

Goodbye to grunt work

Some industry thinking around law and generative AI has been at either end of the spectrum, says Sims. “On the one hand, [it’s] that grads and even lawyers are no longer needed. They are. But not as many will be needed. On the other hand, it’s that AI will have no effect on grads and lawyers because law is ‘special’.”

Neither is correct. Having a good grasp of how to get the best out of generative AI will be beneficial for graduates. Even now, they shouldn’t be doing grunt work, Sims says. “They should never be doing discovery because that’s been done by AI for a long time.

“[When] doing background research for the partner they’re working for, they need to be using the AI tools and other tools to do their work. They’ll be able to do more and, hopefully, more interesting things than they currently are.”

What’s more, the ability of technology to change legal work is not new, she adds. “About 10 years ago, I was at a law and tech conference in Sydney. At my table was a lawyer in his 60s. He said he had changed his practice. He now had seven younger people working for him and was getting through more work than when he had 21 lawyers.”

The only difference is that the pace of change is becoming far more rapid.

Law firms have a couple of years up their sleeves before AI ‘cheats’ start applying for jobs. Students finishing this year or the next have probably done most of their work and assessments without the help of ChatGPT, Sims says.

Going forward, the answer to

worries about so-called cheating could be quite simple. Law firms could reduce their reliance on official academic transcripts and focus more on students proving themselves as interns or summer clerks, she says. It’s a try-before-you-buy approach to employment.

Another alternative might be to use interviews to assess the graduate’s legal knowledge.

It might, in fact, mean those destined to be put out to pasture might be those doing the interviewing, if they can’t keep up with the technology.

“I do know that there are senior lawyers who are very much looking forward to retiring or retiring slightly early, because they can see what’s coming,” Sims says.

On the other hand, while partners may be wringing their hands, the technology will prove useful – at least for those with the skills to harness it and ensure that results are reliable.

For example, Andrew Perlman, dean of Suffolk University Law School, wrote a 14-page legal article in one hour by collaborating with ChatGPT. Summarising the experience, he said: “For the legal industry, ChatGPT may portend an even more momentous shift than the advent of the internet.”

In the right hands, generative AI can be more reliable than lawyers and is highlighting that humans make just as many or more mistakes than machines, Sims says. In the future, she believes it will be negligent not to use AI.

Humans make mistakes

As it stands, ChatGPT has a growing reputation for making up references. In the wrong hands, it’s more of a toy than a tool. Relying on

it in the law is currently risky.

“The results from the generative AI tools are simply not good enough for the results to simply be relied upon,” Sims says. “You need someone with knowledge/expertise to know what is correct and what requires changing, especially with New Zealand law.”

“Knowing what prompts to use works only if you have the ability to judge what is and isn’t correct. This is where knowledge comes in. The ChatGPT comes up with a case. It may be an actual case. But it may have got that case wrong.”

She cites one example she saw in academia where a student entered a question into AI and received an answer containing inaccuracies. Knowing this, the student refined the question two more times until the answer was accurate. The skill was in knowing how to use the tool to fast-track the work. The more desirable graduate will be one who can use the technology in this way.

Lawyers shouldn’t jump into using generative AI without considering the risks. Sims warns lawyers to be very careful about entering client data into public tools such as ChatGPT. “There are all sorts of confidentiality issues there. The reason for that is that [the client data] then becomes part of the data that ChatGPT is using.”

“That’s actually a policy that law firms, if they haven’t done already, need to implement immediately.”

The technology will be integrated into legal solutions, intranets, or other closed systems that keep the information secure, she says.

Policy questions

- What will be the practical implications for Law Firms of AI?
- How will it affect their recruitment and how will junior lawyers be trained in future if AI is doing the research and providing memos?
- What are the risks associated with using AI for firms to consider?

