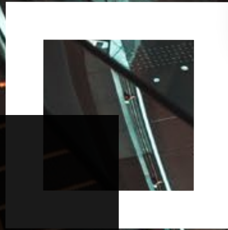


REFLECT

PROTECT

ADVANCE

Litigation Forecast 2024

Shaping New Zealand's future

MinterEllisonRuddWatts.

Contents

02 Introduction

03 Environmental, social and governance (ESG)

04 Come hell of high water: A climate change litigation and greenwashing update

09 Regulatory focus

10 Litigation arising from sanctions: Global sanctions regimes increasing impact on international business

13 FMA's regulatory priorities and financial litigation themes

16 The kōrero continues: Recognition of tikanga Māori by New Zealand courts

18 An ever evolving workplace

19 Changes in the workplace impacting business

21 Cyber and generative AI

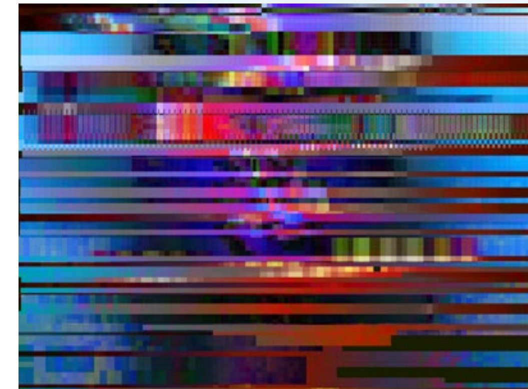
22 Cyber risk and litigation: Some guidelines for directors and boards

27 Navigating the legal minefield: Generative AI and its implications for businesses and directors

31 Health and safety

32 Health and safety prosecutions: The outlook post-Whakaari White Island

34 Our Litigation and Dispute Resolution team



Introduction

As each new year starts, it seems that life gets more complex, with new challenges and opportunities to navigate. New Zealand's evolving litigation landscape is no different.

Litigation reflects the biggest issues facing New Zealanders today, and into the future – highlighting the things we care about most.

This year's Litigation Forecast provides an update on the challenges of climate change litigation and greenwashing, sanctions litigation, and the changes in the workplace impacting on business. We also discuss the ongoing recognition of tikanga Māori as a source of law by the New Zealand Courts.

Turning to technology, we examine the complexity of cybersecurity risks and discuss generative AI and the implications for directors and boards.

Finally, we also look at the impact of the Whakaari | White Island proceedings following the devastating eruption in 2019.

However, the more things change the more they stay the same. Excellent legal advice, industry knowledge and expertise, astute strategic and procedural thinking and superb client service remain at the heart of dealing skillfully with litigation risk.

Our Tier 1 Litigation and Dispute Resolution team has long-standing experience navigating New Zealand's most important litigation, and was in the thick of last year's largest and most complex cases.

With an eventful year projected by many economic analysts, we are eager to continue supporting clients through 2024 and beyond.

Environmental, social and governance (ESG)

Come hell or high water:

A climate change litigation and greenwashing update

Climate change litigation is a developing frontier. Activists are increasingly turning to the courts to hold to account those perceived as directly or indirectly contributing to climate change. This article focuses on the complex matrix of liability for private companies as well as the latest trends in climate change litigation and greenwashing around the world.

The Supreme Court's decision in *Smith v Fonterra* – a landmark judgment of international significance to large corporates

The Supreme Court of New Zealand this month handed down a landmark decision in *Smith v Fonterra & Ors*, allowing claims brought by a climate change activist against seven corporate defendants to proceed to trial. The decision marks a significant departure from the approach taken by the Court of Appeal, which had earlier agreed with the defendants' arguments that the claims should be struck out because they had no prospect of success.

The Supreme Court's decision is important because it marks a rare success by an activist litigant against a corporate defendant in a climate change case in a common law jurisdiction. It opens up the possibility of other activist litigation against corporate defendants relating to their carbon emissions or other aspects of their operations that may have an adverse environmental effect. While such claims may not have any real prospect of success at trial, the decision means that it will be more difficult for corporates to use the summary strike-out procedure to bring them to an end quickly and efficiently.

The plaintiff, Mr Smith in *Smith v Fonterra & Ors* is an elder of Ngāpuhi and Ngāti Kahu and a climate change spokesperson for the Iwi Chairs Forum. He claims a traditional connection to coastal land which he says is threatened by climate change. He brought his claims in the torts of public nuisance, negligence and a proposed new tort relating specifically to climate change.

The argument before the Court related primarily to the tort of public nuisance, which in general terms applies where a person allows an emanation from their land to affect the property of another person to their detriment.

In finding that the claims ought to be permitted to proceed to trial, the Court addressed the following key issues which will be relevant to other climate change litigation:

1. **Novel claims may be harder to strike out:** The novel nature of the claims and the significance of the harm claimed militated against permitting them to be struck out without a full trial, where a decision could be made with the benefit of evidence and full argument. This may encourage other activist litigants to push boundaries with new types of claims.

2. **Legislative action does not exclude common law claims:** Legislative regimes intended to provide a comprehensive national response to the challenge of climate change, such as permit regimes for emissions and carbon credits under enactments such as the Climate Change Response (Zero Carbon) Amendment Act and Resource Management Act, do not exclude the possibility of common law claims. An emitter that has been granted permission to operate within certain parameters under the legislative scheme may nevertheless be challenged by an activist litigant. This may encourage activists who consider that the Government's response does not go sufficiently far.

3. **Causation not fatal:** The challenge for the plaintiff of proving that the defendants' emissions (or emissions by others that they facilitate) caused him specific loss notwithstanding that they are only a tiny proportion of global emissions was not fatal to his claim. The Court made reference to old cases in which polluters of rivers were held liable for damage suffered by other users of the rivers, notwithstanding that other persons were also causing pollution, although in those cases the connection was more obvious and direct. The plaintiff's requirement to prove 'special damage' in a claim of public nuisance was not a bar to his claim.

4. **Only "substantial and unreasonable" emitters will be caught:** The claims will only succeed if the plaintiff proves that the defendants' actions amounted to a "substantial and unreasonable" infringement of his rights, which is a "significant threshold" that only some emitters will cross. Those who merely drive cars or heat their homes, for instance, will not be caught. This creates an interesting distinction between those who drive cars or heat their homes and those who supply them with the fuel that enables them to do so, albeit the end result is the same. However, the Court held that whether the defendants' conduct exceeded this threshold could only be determined at trial.

5. **Remedies may not be effective:** Of some comfort to corporates who are prospective targets of these claims, it was far from clear that a remedy of any significance would be granted even if the plaintiff succeeded in proving a breach of a legal duty. The Court indicated that the case might be legally untenable if the plaintiff claimed money damages to compensate him for loss, as a "more conventional" approach might then be taken to the requirement for proof of causation. However, he was seeking only declarations and injunctions. The declarations sought were a possible remedy, although the claim for injunctions faced obstacles and the Court would tailor any injunctions with a view to their impact.

6. **Tikanga Māori:** The Court acknowledged that tikanga was relevant to the claim and that aspects of tikanga would need to be addressed at trial, particularly in relation to the plaintiff's claimed relationship with the relevant land and claims to be exposed to loss and damage in ways that are not necessarily financial or economic.

The decision is of importance to large corporates that are significant greenhouse gas emitters or support or facilitate other concerns that are significant emitters, as it exposes them to the prospect of activist litigation on novel grounds. While such litigation may have limited prospects of success at trial, and even if there is a measure of success the remedies granted may have limited effect, the litigation process can be public, slow and expensive. Activists may be encouraged by the decision to identify new opportunities to raise the public profiles of their causes and put pressure upon corporate actors with more confidence than before.

The case will now be scheduled for a trial in the High Court in the usual way.

Disclosure: MinterEllisonRuddWatts' Auckland and Wellington litigation teams separately represent two of the defendants in the proceeding.

Climate change trends in Australia and the United Kingdom

Globally, regulators, NGOs and climate change activists are sharing experiences and learnings across different jurisdictions to adapt their proceedings to achieve their desired outcomes. New Zealand businesses therefore need to keep a sharp eye on overseas precedents and how those might encourage litigation trends in New Zealand.

On a per capita basis, Australia is a global leader in climate change litigation, second only to the United States. While New Zealand has already seen some climate change litigation, there is much to be learned from Australia, the United Kingdom and Canada.

The Australian regulators have been active, with ASIC issuing three proceedings for alleged greenwashing by several superannuation funds.[1] On 12 December 2023, following the Australian Competition and Consumer Commission's (ACCC) review of greenwashing claims, it released eight principles to guide environmental claims in marketing and advertising, emphasising the need for accurate, evidence-based, clear messaging in respect of environmental claims.[2]

Cases in the United Kingdom last year have also demonstrate a novel pathway for plaintiffs to challenge how companies assess and address climate risks – targeting directors personally). If we see successful litigation of this nature globally, the implications for D&O insurance, corporate decision-making and risk management could be significant. The introduction of New Zealand's new Climate-related Disclosures regime, with reporting due from 2024, will also set the foundations for future actions to come, as seen overseas.

Greenwashing action: not a matter of if, but when

Greenwashing penalties pose one of the greatest risks to private entities arising from climate-related obligations. While the law behind "greenwashing" is essentially governed by the concept of misleading and deceptive conduct in the Fair Trading Act 1986 and the fair dealing provisions of the Financial Markets Conduct Act 2013, the application of that law is far from simple. This is particularly evident in enterprise branding. While a company can make a statement about its environmental credentials which, on its face is true, it could be considering misleading and deceptive if it causes a misleading impression overall.

A key example of this is the UK Advertising Standards Authority's (ASA) decision in October 2022 relating to HSBC UK Bank plc (HSBC UK). In that decision, the ASA considered two statements made by HSBC UK on bus shelters: "*HSBC is aiming to provide up to $1 trillion in financing and investment globally to help our clients transition to net zero*" and "*[W]e're helping to plant 2 million trees which will lock in 1.25 million tonnes of carbon over their lifetime*". While both statements were true, the ASA concluded that a consumer would form the view that HSBC UK was making a positive overall contribution to the environment, that it was committed to ensuring its business and lending model would help support businesses to transition to net zero, and that planting two million trees would be a meaningful contribution to the sequestration of greenhouse gases. The ASA considered this impression was misleading where HSBC UK was financing companies that generated notable levels of emissions and intended to keep funding thermal coal mining and power production to 2040. This decision was not without controversy, but the ASA's guidance doubled down on this holistic view.[3] While the ASA decision is not binding on any New Zealand court, we expect that the country's regulators will be alive to this approach and may take a similar view.

1 Mercer Superannuation (Australia) Limited, Vanguard Investments Australia and LGSS Pty Limited (ActiveSuper).

2 Australian Competition and Consumer Commission " ACCC releases eight principles to guide businesses' environmental claims" (press release, 12 December 2023).

3 Committee of Advertising Practice *The environment: misleading claims and social responsibility in advertising — Advertising Guidance (non-broadcast and broadcast)* (Advertising Standards Authority, June 2023).

To be prudent, any statement relating to sustainability, climate change or environmental credentials needs to be not just factually correct, but checked for any overarching impression the statement might create in the minds of consumers.

Climate change action against directors

In England, two cases in 2023 opened the gateway for action against directors personally for breaches of directors' duties. The director's duty to act in the best interests of the company in the Companies Act 2006 (UK) now includes mandatory ESG considerations, which have underpinned these novel actions. New Zealand's newly amended equivalent duty in the Companies Act 1993 does not go this far, only making ESG considerations voluntary (as in the Canadian Business Corporations Act 1985), but there is scope for ambiguity in how much attention must be paid to these non-mandatory considerations. As the Australian Institute of Company Directors has repeatedly emphasised, climate risk is financial risk and will inevitably colour how directors discharge this duty.[4]

In May 2023, the English High Court dismissed a derivative action by ClientEarth, a shareholder of Shell plc, against the company's directors in the novel case of *ClientEarth v Shell plc*.[5] ClientEarth alleged that Shell's directors were in breach of their duty to act in the best interests of the company, which includes having regard to the company's impacts on the community and environment, by failing to properly address the risks of climate change through Shell's operations. The High Court reaffirmed the careful balancing act of considerations required of directors, especially large multinationals, and that the Court is slow to interfere with this balance unless there is a clear breach of the duty. The Court was also skeptical of ClientEarth's good faith in bringing the claim as a minority shareholder and as an activist organisation whose values were opposed to Shell's operations. On that basis, ClientEarth was also required to pay costs.

Soon after the ClientEarth decision, in July 2023, the English Court of Appeal heard a similar line of argument in *McGaughey v Universities Superannuation Scheme Ltd*.[6] Several members of a pension scheme brought a derivative action against the directors of the corporate trustee who administered the scheme, alleging their investments did not align with many decarbonisation and divestment goals. The Court of Appeal agreed with the High Court that this was not a derivative action because there was no loss suffered and no breach of any directors' duties was alleged.

The English courts have shown they are slow to interfere in director decision-making that has impacts on climate risks, especially considering the variety of competing and often polarised considerations they are required to balance when acting. Nevertheless, the potential to sue directors personally for their actions on behalf of the company is now in the minds of shareholders.

While ESG considerations are not mandatory for directors discharging their duty of good faith in New Zealand, providing a further buffer against such claims, this area could develop quickly if majority shareholders also begin to challenge director decision-making and tangible losses could be proven.

The best way to guard against such action is to ensure that the board's decisions on climate change are robustly considered with external evidential support to substantiate them, that goals are clearly communicated and achievable and, if the company's ability to reach its goals is compromised, the company ensures it communicates this to stakeholders clearly and in a timely manner.

4 Noel Hutley and Sebastian Hartford-Davis *Climate Change and Directors' Duties: Memorandum of Opinion* (The Centre for Policy Development and the Future Business Council, 7 October 2016); and Gerald Ng *The Content of Directors' "Best Interest" Duty: Memorandum of Advice* (Australian Institute of Company Directors, 25 July 2022).

5 *ClientEarth v Shell plc* [2023] EWHC 1137 (Ch);*ClientEarth v Shell plc* [2023] EWHC 1897 (Ch); and *ClientEarth v Shell plc* [2023] EWHC 2182 (Ch).

6 *McGaughey v Universities Superannuation Scheme Ltd [2023] EWCA Civ 873, [2023] Bus LR 1614.*

Climate-related disclosures and the path ahead

With the introduction of climate-related disclosure obligations in the Financial Markets Conduct Act, 2024 will be the first financial year when climate reporting entities will need to prepare and lodge climate statements. New Zealand's new climate-related disclosures framework reflects similar disclosure regimes in other jurisdictions where regulators or shareholders have brought actions for insufficient disclosures, indicating similar actions could arise in New Zealand.

Liability for failure to comply with climate standards can fall on climate reporting entities and their directors, and fines or civil penalties can reach up to $2.5 million. However, the Financial Markets Authority (FMA) has indicated that a limited grace period will apply at the beginning while companies navigate their new obligations. As this will not last forever, many companies are working on voluntary disclosure to ensure that teething issues are well addressed by the time the FMA seeks to use its enforcement tools.

While regulators will have their eye on compliance with climate-related disclosure obligations, shareholders will too. Australia has seen shareholders scrutinise financial institutions for failing to make accurate and transparent disclosure of climate risks. In *McVeigh v Retail Employees Superannuation Trust* (REST), a pension fund member sued REST alleging it had failed to disclose information about climate change-related business risks and plans to address them. The claim was ultimately withdrawn, but only once REST agreed to implement climate targets and measure, monitor and report its progress according to the recommendations of the Task Force on Climate-related Disclosures. Furthermore, in *Abrahams v Commonwealth Bank of Australia*, the Federal Court of Australia granted orders permitting a shareholder of the Commonwealth Bank of Australia access to internal documents to assess the bank's compliance with its environmental policies and commitments.

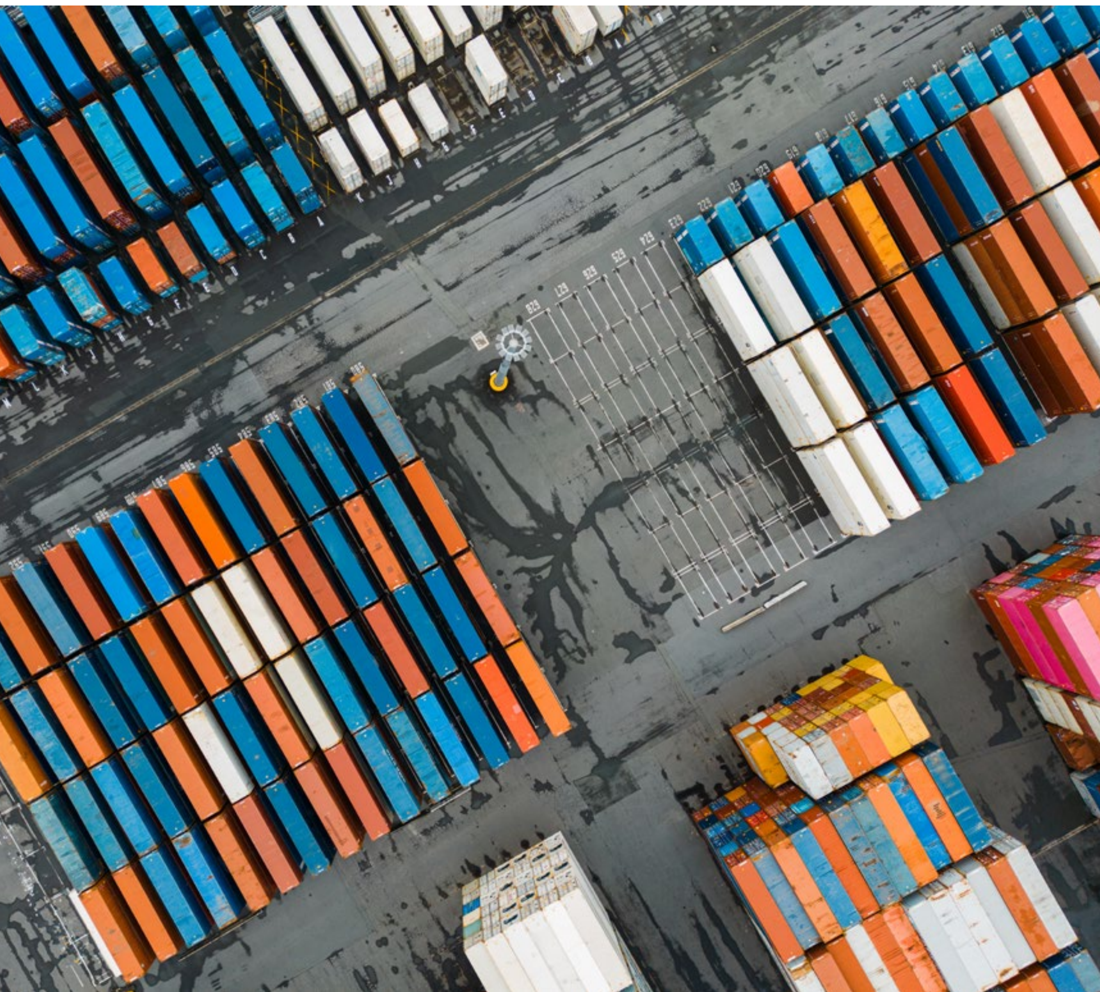
With similar procedures available under the Companies Act 1993 in New Zealand, companies should be aware of the potential for the Court to intervene and require disclosure if shareholders are not getting the full picture on climate risk assessment and mitigation plans, as in Abrahams.

Transparency and accuracy will be key to avoid action both from regulators and shareholders on climate-related disclosures.

2024 and beyond

The repurposing of existing causes of action and the creation of novel types of proceedings is set to continue as individuals, shareholders and NGOs draw inspiration and learn from litigation around the world. We expect to see new areas of focus such as biodiversity conservation, ocean protection and water scarcity. A complex patchwork of liability awaits companies as they seek to navigate this evolving area.

Regulatory focus



Litigation arising from sanctions:

Global sanctions regimes increasing impact on international business

Economic sanctions have been proliferating in recent years and have been subject to unprecedented development since Russia's invasion of Ukraine in February 2022.

Given the reliance of New Zealand's economy on importing and exporting goods and services, businesses are constantly having to grapple with the implications of dealing with overseas counterparts in an increasingly fractious world. With geopolitical tensions continuing to rise and geoeconomic fragmentation in the face of slow economic recovery, we predict that sanctions compliance and enforcement will continue to be a hot topic in the year ahead.

The rise of sanctions regimes at home and abroad

Sanctions are used internationally to apply pressure to countries, regimes, companies and individuals that threaten peace and security, have harmful policies or do not comply with international law.

As a Member State of the United Nations (UN), New Zealand is required to implement sanctions resolutions passed by the UN Security Council. Generally, these resolutions have been the sole driver of sanctions implementation in this country. However, following Russia's veto of UN sanctions in response to the invasion of Ukraine, Parliament passed the Russian Sanctions Act 2022 and associated regulations that place a range of obligations on all New Zealanders by prohibiting or restricting specific activities, and requiring the reporting of suspicious activity.

The introduction of Russian sanctions is of interest in two respects:

- it creates compliance obligations and exposure for any business or individual interacting with Russian interests; and
- it potentially signals a new direction in New Zealand's foreign policy and the potential growth of an autonomous sanctions regime, rather than the historical approach of keeping in step with the UN.

These are both issues that business will have consider when interacting with foreign counterparts.

Relevance of international events to businesses down under

Businesses that rely on the import and export of goods, services and capital, are regularly having to assess the ultimate source of funding, commodities and 'control' in transactions. This is not always easy to discern and deciphering the do's and don'ts of a particular sanctions regime can be challenging. Sanctions compliance is a very technical area of the law riddled with complexity.

New Zealand is rich with examples of successful businesses punching above their weight on the world stage. Now, more than ever, those businesses are eager to identify their sanctions compliance obligations and take steps to minimise their exposure to sanctions-related risks, including by implementing a Sanctions Compliance Policy. Especially for businesses dealing in or with:

- **high-risk sectors:** financial institutions, investors, importers, exporters and logistics providers, defence and aerospace businesses, technology and telecommunications companies; energy and natural resources companies; multinationals; and professional services firms; or
- **high-risk jurisdictions:** Belarus, Cuba, Iran, Myanmar, North Korea, Russia, Sudan, Syria, Venezuela and the Ukrainian regions of Crimea, Donetsk, and Luhansk.

But it is not just an individual business's exposure that is relevant when considering sanctions compliance. In fact, often, one of the primary considerations is how international counterparts may perceive your actions and whether they present a compliance risk by association. If you are dealing with entities in countries with particularly assertive regulators (such as the Office of Foreign Assets Control in the United States) their risk appetite will matter just as much as your own.

A recent illustration: New Zealand's Russian "oligarch" litigation

Last year, MinterEllisonRuddWatts represented Westpac New Zealand Limited (Westpac) in successfully defending an injunction application brought by Targa Capital Limited (Targa) to force the bank to continue providing services in circumstances where it was not satisfied that Targa was not ultimately controlled by a sanctioned individual, Alexander Abramov.[1]

The bank pointed to three key risks justifying its decision to close Targa's accounts: regulatory; contract and capital markets risk. The extraterritorial scope of UK and Australian sanctions regimes created compliance risk for related group entities registered or carrying on business in the UK or Australia, or UK or Australian nationals employed by Westpac. The High Court considered that the UK sanctions regime in particular has wide "real world" test of control such that it was reasonable to be concerned that Mr Abramov could still ensure Targa's affairs were conducted in accordance with his wishes notwithstanding attempts to structurally remove him from the Trust that controlled Targa.

Ultimately, the High Court judgment confirmed a bank's right to terminate its relationship with a customer upon reasonable notice, subject to the terms of the contract between the parties. But critically, for present purposes, it also confirmed that, when deciding whether to exit a customer, a bank is entitled to have regard to its own commercial interests and its desire to manage sanctions risks. In particular, Westpac's assessment of its exposure to risk from continuing its relationship with Targa was not unreasonable given its limited control on how third parties perceive the risk of sanctions breach or react to that perception.

Sanctions sub-plot: The rise of de-banking

The sanctions issues in this case were intertwined with another issue which is the subject of increasing scrutiny around the world: de-banking.

De-banking refers to the practice of a bank or financial institution terminating or restricting its relationship with a customer.

Although not the subject of this article, since the decision in *Targa v Westpac* there have been two further, high-profile decisions related to de-banking: one in the context of human rights breaches and ESG policies (*The Christian Church Community Trust v Bank of New Zealand* [2023] NZHC 2523) and the other arising from concerns related to the AML/CFT compliance of money remittance companies (*The Ink Patch Money Transfer Limited v Reserve Bank of New Zealand* [2023] NZCA 587).

This is another area to watch and which is garnering attention internationally. Take for example, the resignation of the CEOs of the British bank, NatWest, and a subsidiary private bank, Coutts, after it terminated its relationship with prominent political figure Nigel Farage. Documents obtained by the individual revealed that, while he had for some time been below its commercial criteria – requiring customers to have £3 million in savings or £1 million in loans or investments – Coutts was ultimately concerned that his alleged "xenophobic, chauvinistic and racist views" posed a risk to the bank's reputation.

As the *Targa v Westpac* decision illustrates, there will often be an interplay between sanctions and the termination of contractual arrangements. However, there will also be frequent occasions on the margins, (i.e. where a sanctions or other legal overlay has not been clearly triggered but one party is uneasy about its continued relationship with the other.) In the case of sanctions on high-net-worth individuals, there is growing recognition of the sophistication of arrangements used to obfuscate the beneficial ownership of assets and sources of funds (e.g. through trusts, protectorships, side arrangements and influence over public facing individuals).

Crystal ball gazing for managing compliance and enforcement risk

Doing business may be getting harder, especially with international counterparties. However, a National-led coalition government is expected to prioritise trade as a means for boosting the country's economic growth. Given the National Party and the Act Party have both historically favoured the establishment of an autonomous sanctions regime to support independent foreign policy, it will be interesting to see how the coalition government balances sanctions implementation with its pro-business policy agenda. Regardless, we expect to see increasing scrutiny by the legislature, regulators and business going forward.

1 *Targa Capital Limited v Westpac New Zealand Limited* [2023] NZHC 230.

FMA's regulatory priorities and financial litigation themes

The regulation of financial markets is constantly evolving to respond to a changing environment. Recently, we have seen heightened geopolitical uncertainty, market volatility, and unpredictability in the global economy. Financial markets are also becoming increasingly fragmented and digitised.

Change has been the only constant over the last few years, with the roll-out of regulatory reforms following the Conduct and Culture reviews of banks and life insurers in 2018 and 2019. While some of these reforms are at the implementation stage, others are yet to come into force. For example, the new regulatory regime for financial advice came into effect in March 2023, capping off a transition that began in 2019. In the last year, the Financial Markets Authority (FMA) engaged on and published guidance on the Climate-related Disclosures regime to help entities get ready for the first year of reporting in 2024, as well as the Conduct of Financial Institutions (CoFI) regime, currently due to come into force in March 2025. However, the formation of the new Coalition Government in New Zealand has thrown uncertainty on the future of some of these regulatory reforms. We summarise the changes at the end of this article.

Against this backdrop of change and uncertainty, we examine the current regulatory trends and priorities of the FMA.

FMA's strategic priorities

Outcomes-focused regulation

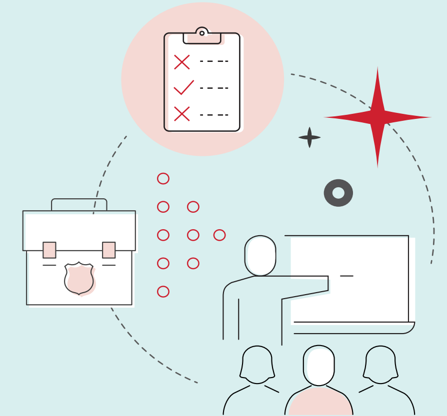
Clare Bolingford, Executive Director of Regulatory Delivery at the FMA, indicated in August 2023 that the FMA's first key priority is to develop a more outcomes-focused approach to supervision and monitoring.[1] A few months later, in November 2023, the FMA released a draft guide on its approach to outcomes-focused regulation for consultation, with a specific focus on fair outcomes for consumers and markets by financial service providers.

Earlier this year, Minister of Commerce and Consumer Affairs Andrew Bayly affirmed the importance of fair conduct and stated that businesses that have begun preparing fair conduct programmes (FCP) in anticipation of CoFI's implementation should continue to do so. The confirmation provided by Minister Bayly means that this consultation is key for the future delivery of financial services and for enforcement.

The consultation guide (which can be found here) reflects the FMA's expectation that firms will focus on results and move away from compliance as a matter of form and prescription. It sets out seven "fair outcomes" that the FMA considers firms should be working towards:

1. Consumers have access to appropriate products and services that meet their needs;
2. Consumers receive useful information that aids good decisions;
3. Consumers receive fair value for money;
4. Consumers can trust providers to act in their interests;
5. Consumers receive quality ongoing care;
6. Markets are trusted based on their integrity and transparency; and
7. Markets enable sustainable innovation and growth.

Consultation closes on 1 March 2024, after which the FMA will review submissions and finalise the fair outcomes and guide.



FMA's strategic priorities

Outcomes-focused regulation

Improving understanding of the drivers of market, provider, and consumer behaviour

Taking a proactive approach to minimising harmful conduct on the perimeter

Deterring misleading value propositions

1 Clare Bolingford, FMA Executive Director of Regulatory Delivery (speech at 2023 Financial Services Council Conference – 16 August 2023): See also the FMA Outlook 2023/2024

In her 2024 FSC speech, Samantha Barrass, the FMA Chief Executive, emphasised that using the core principles at the heart of CoFI can result in a simple and streamlined approach for conduct regulation. Further to the Minister's indication that the Government wished to transfer responsibility for monitoring CCCFA conduct from the Commerce Commission to the FMA, Barrass noted that aligning credit regulation with an outcomes-based approach and fair conduct rules would provide regulatory certainty and efficiency. For example, the FMA may turn to the Financial Markets Conduct Act to support appropriate regulation of registered banks, non-bank deposit takers and high-interest rate lending, particularly those targeted at vulnerable communities.

Improving understanding of the drivers of market, provider, and consumer behaviour

The FMA's second strategic priority is to improve its understanding of the drivers of market, provider, and consumer behaviour by gathering evidence, insights and data from firms and other regulators.[2]

Bolingford has said that this will help to establish *"an evidence base to decide where to focus [the FMA's] discretionary effort; a feedback loop to evaluate the impact of those actions; and core intelligence data to improve [its] practice"*.[3] Also relevant is that the FMA has appointed a Chief Economist for the first time. Barrass said that the role would assist in focusing *"our regulatory lens on the right priorities and outcomes"* and that it would make a *"significant difference to the way we best target our resources"*.[4]

Taking a proactive approach to minimising harmful conduct on the perimeter

The Financial Markets Conduct Act 2013 (FMCA) established what the FMA calls its perimeter – the borderline of its formal powers. The FMA has indicated that its third strategic priority is to focus on activity on the perimeter that causes harm to the public and erodes confidence in the system.[5]

In recent years, following the Conduct and Culture reviews of banks and life insurers, the FMA has focused on customers being overcharged or otherwise disadvantaged as a result of poor practices and inadequate systems and processes. This has resulted in seven civil proceedings of this nature against banks or insurers, including the largest penalty to date of $3.9 million. These cases provide lessons in how the courts view the application of the fair dealing provisions, and important guidance for firms on conduct and the need to invest in appropriate systems and controls.

Further, in May 2023, the FMA issued a permanent stop order to Validus and Associates, which is registered in the United States, for making misleading offers of financial products that did not exist. This shows that the FMA will take steps to challenge unregulated harmful activity even when it originates overseas.

Criminal activity that causes harm to the public, such as scams and frauds, also sit on the perimeter. In recent years, there has been a global surge in scams and crimes targeting the financial sector. As with the International Organisation of Securities Commissions, the FMA has raised this issue to the top of its agenda. The New Zealand Banking Association also announced in September 2023 that it was going to investigate improving the industry scam response, including introducing name and account number checking.

Deterring misleading value propositions

The FMA's fourth strategic priority is deterring misleading value propositions of financial products and services.[6] This includes a focus on inappropriate advertising, issues with multi-policy discounts, value for money, poor disclosure, and increasingly under CoFI, the design and distribution of everyday financial products.

Over the last few years, the FMA has brought penalty proceedings against five entities for insurance relying on the fair dealing provisions. Penalties of up to $3.9m were paid. We can expect this trend to continue.

Similarly, in recent years, Australian Securities & Investments Commission (ASIC) has focused on failures by insurers to deliver on their pricing promises, resulting in the Federal Court of Australia imposing the highest penalty of $40 million in June 2023. In 2024, ASIC has indicated that it is turning its attention to failures in insurance claims handling, with a focus on claims handling, poor communication and record keeping, and inappropriate use of exclusions.[7] ASIC

2 Clare Bolingford, above n 1
3 Clare Bolingford, above n 1.
4 FMA appoints Stuart Johnson to new Chief Economist role
5 Clare Bolingford, above n 1.
6 Clare Bolingford, above n 1.
7 Sarah Court, ASIC Deputy Chair (speech at ASIC Annual Forum 2023 – Enforcement session opening remarks, 21 November 2023)

ASIC has noted that for consumers in the unfortunate situation of needing to claim on their insurance policy, timely and fair claims handling is crucial.[8] We expect this to be a key theme in New Zealand in the years to come. In the 2022/2023 FMA annual report, Samantha Barrass reiterated the FMA's continual expectations for insurers to resolve claims in a manner that is fair and timely, putting the interests of each customer at the centre of their response.[9]

Final remarks

As ASIC Chair Joe Longo indicated, the need for change is constant, and to remain effective, regulators must be open to change themselves.[10] The FMA is adjusting their regulatory and enforcement approach to respond to changes in the financial, economic and political environment. It is important for firms to keep up with regulatory trends and priorities to ensure they are meeting changing regulatory expectations.

8 Sarah Court, ASIC Deputy Chair (speech at ASIC Annual Forum 2023 – Enforcement session opening remarks, 21 November 2023)
9 FMA 2022/2023 Annual Report, at 9
10 As above

Financial Services Council (FSC) Outlook 2024: Changes to financial regulation

At the FSC Outlook 2024, the new Minister of Commerce and Consumer Affairs, Andrew Bayly, stated that the complex legislative and regulatory framework currently governing the financial services sector has led to lack of clarity and increased operational costs. He signalled an intention to simplify this framework to reduce compliance burden without comprising the protection of consumers' interests. Samantha Barrass also spoke at the FSC 2024 Outlook event and indicated her alignment with the Minister's key messages. The Minister and Ms Barrass' speeches can be found here and here respectively.

CoFI regime

Minster Bayly signalled that a targeted reform of CoFI, rather than a repeal, was appropriate, to ensure that good conduct obligations are proportionate and fit-for-purpose. The reform includes two aspects:

- it will reinforce the principle that the responsibility for determining what is an appropriate fair conduct programme for their specific business lies with the applicant. This means that liability lies with the directors and management and the board to identify key risks in areas of concern and develop their fair conduct programmes accordingly.
- the FMA is expected to issue clear guidance for smaller institutions to meet minimum requirements of conduct.

At the same time, Minister Bayly affirmed the importance of fair conduct and stated that businesses that have begun preparing fair conduct programmes (FCP) in anticipation of the regime's introduction should continue to do so. In terms of the FMA's expectations of FCPs, Samantha Barrass has emphasised that it is not the FMA's intention to scrutinise FCPs line by line during the licensing process, and that FCPs should be right-sized for the businesses they serve. Ms Barrass indicated that the FMA will be flexible and respond to different business models in their licensing, supervision and monitoring approach, rather than using a 'tick box' approach.

Credit Contracts and Consumer Finance Act 2003 (CCCFA)

Minister Bayly stated that a priority was to reform the CCCFA to protect vulnerable consumers without unnecessarily limiting access to credit. In his view, the current detailed regulations and strong liability regime have led to overly risk-averse lending decisions, created unnecessary compliance costs, and reduced access to credit for consumers.

As a starting point, he proposed removing the prescriptive affordability requirements for lower-risk lending. From there, he proposed undertaking a more substantive review of the CCCFA, including reviewing its penalty and disclosure regime, and its relationship with the CoFI regime.

Twin peaks regulatory model

The Minister also spoke to the significance of the twin peaks regulatory model. He supported maintaining a clear distinction between the purview of the Reserve Bank of New Zealand as prudential regulator and the FMA as conduct regulator. To that end, he proposed the following changes:

- Transferring responsibility for monitoring conduct in respect of the CCCFA from the Commerce Commission to the FMA;
- Consolidating and simplifying existing conduct licensing requirements (for example, the FMA could issue a single licence covering conduct issues for financial institutions); and
- removing duplication in areas of initial fit-and-proper person assessments and cyber resilience reporting.

The kōrero continues:

Recognition of tikanga Māori by New Zealand courts

The momentum has continued in 2023, following the landmark Supreme Court decision in the Ellis case at the end of 2022[1], for increasing recognition in litigation of tikanga Māori as part of New Zealand law. This recognition is occurring through application of Te Tiriti o Waitangi clauses in statutes[2], application of direct reference to tikanga and tikanga principles in statutes, and through evolution of the common law. In parallel, parties to litigation are increasingly drawing on tikanga and Te Tiriti-based arguments as a possible basis for a claim or defence.

Looking ahead to 2024, while the new Coalition Government has put debate about the principles of Te Tiriti squarely on the political and policy agenda (through the coalition agreements), we expect the slow but steady recognition by our courts of tikanga as a part of New Zealand law, with its own legal force, to continue unabated.

The release of the Law Commission's *He Poutama* Study Paper 24 in September 2023 is a clear reflection of this momentum[3]. *He Poutama* provides an extensive account of what tikanga is and how tikanga and state law might best engage. It highlights the existing breadth of application of tikanga as part of New Zealand law[4]. As well as detailing the development of tikanga as part of the common law, as statute law, and as law and custom applicable in its own right, *He Poutama* details the significant volume of litigation (and expert evidence) that is seeking to engage with tikanga values and processes in areas as diverse as environmental law, criminal law, family law, and judicial review of public sector actions and decision making.

There is much we could focus on in this area from the last 12 months. One developing field has been litigation involving application of tikanga in what are essentially commercial transactions. In 2023 the High Court engaged with arguments based on tikanga principles in relation to a case involving an application by the Official Assignee for a possession order over land following bankruptcy of the owners. The owners had sought to transfer the land to a whanau trust and argued that tikanga would require that the creditors sit down and engage with them to resolve the matter with whanau, rather than make a possession order. The High Court held that tikanga could not be applied to override the effect of the Insolvency Act in that case, but that tikanga may nevertheless be relevant to the parties separately engaging and seeking to find a resolution to the matter.[5]

Another case which drew on tikanga arguments in 2023 involved the repayment of a judgment debt to a Māori land trust, where the defendant argued (among other things) that the Court should not exercise its discretion to grant leave for enforcement proceedings based on application of tikanga principles. The High Court engaged extensively with whether tikanga was relevant (holding that it was), and on how it would affect the Court's discretion in that case. Ultimately, the Court held that, contrary to the defendant's position, there are many relevant tikanga principles (the defendant could not pick and choose that suited their case), and those principles were in fact consistent with enforcement in this case. Leave to commence enforcement proceedings was granted.[6]

Another significant development in 2023 (albeit currently under appeal to the Supreme Court) was the jurisdictional change from the Māori Land Court into the High Court for cases involving Post Settlement Governance Entities (PSGEs) set up as discretionary trusts (trusts established to hold and manage Ti Tiriti settlement redress on behalf of iwi and hapu) when the discretionary trust is established to hold and manage a range of assets, rather than only land. In *Kruger v Nikora*[7], a case involving an application filed with the Māori Land Court regarding the Tūhoe Te Uru Taumatua Trust, the PSGE for Ngāi Tūhoe, the Court of Appeal held that the Māori Land Court did not have jurisdiction to grant orders in relation to that post settlement governance entity as it was not a trust constituted in respect of general land owned by Māori per s 236 of the Te Ture Whenua Māori Act 1993.

If the decision is upheld on appeal to the Supreme Court, we may likely see an increase of PSGE litigation (which is often rounded in tikanga based dispute resolution processes) in the High Court which otherwise would have originated in the Māori Land Court. That will raise the ongoing issues and discussion about the interpretation and application of tikanga in the High Court and whether this forum is best suited to respond to such disputes when they arise. The jurisdiction issue is also significant as the Māori Land Court has a broader, more intensive supervisory jurisdiction than the High Court (including in relation to the appointment and removal of trustees) and it can be easier and cheaper for beneficiaries to access the Māori Land Court.

1 *Peter Ellis v R* [2022] NZSC 114.

2 Article 2 of Te Tiriti protects Māori rangatiratanga, which includes chiefly authority and self-determination rooted in tikanga.

3 *He Poutama Study* Paper 24

4 Appendix 2 of He Poutama (see page 17 for excerpt)

5 *Bamber v Official Assignee* [2023] NZHC 260.

The kōrero continues:
Recognition of tikanga Māori by New Zealand courts

Some of the key advances in judicial recognition of tikanga principles in 2023 occurred as part of employment litigation. We have seen an increase in the number of employees challenging the actions of employers who have failed to adequately consider tikanga principles as part of the employment dispute resolution process. There have been both Employment Relations Authority determinations and Employment Court decisions addressing this issue.[8] The general principle arising from these cases is that, where an employer has expressed a commitment to kaupapa Māori and tikanga principles, they are expected – as a matter of contract, of fairness and reasonableness as an employer, of good faith relations, and in the public sector, as a matter of heightened statutory obligation – to act consistently with that commitment in their employment relationships/practices. As we move into 2024, we expect the Employment Court will grapple with this issue further, particularly in the context of good faith duties.

In addition, recognition of tikanga continues to be a key aspect of judicial review of public sector decision making across a wide range of sectors in 2023, and this will almost certainly continue, pending serious legislative change by the current Coalition Government.

As part of these developments, common tensions arise across all areas of litigation involving claims and arguments based on tikanga and application of tikanga principles in our general courts. Key among them is who can and should define tikanga, and to what extent do courts have a role in determining tikanga disputes and a place in recognising and upholding tikanga.

In the Ellis decision, the Supreme Court expressly urged caution, emphasising that it "must not exceed [its] function when engaging with tikanga", and that "care must be taken not to impair the operation of tikanga as a system of law and custom in its own right".[9]

The Law Commission's *He Poutama* paper is intended to help all parties to potential litigation where tikanga principles may be relevant, as well as lawyers and the courts, to gain a common understanding and to find a way through.

For anyone engaging with litigation where tikanga principles are relevant – and we expect to see more of these in 2024 and beyond, and in a wider range of legal contexts – *He Poutama* is likely to become essential reading.

Appendix 2 of *He Poutama* compiles tikanga as expressed in evidence presented in legal proceedings. It includes an explanation of tikanga by Tā Hirini Moko Mead (Ngāti Awa) and Tā Pou Temara (Ngāi Tūhoe) in a joint statement as follows:

"Tikanga is the first law of Aotearoa. It is the law that grew from and is very much embedded in our whenua (land). Tikanga Māori came to the shores of Aotearoa with our Māori ancestors, starting with Kupe and those on board the waka (canoe) Matahourua. In some traditions, tikanga merged with that already present. Tikanga operated effectively for around a millennia before Pākēha arrived. Tikanga is the Māori "common law". It is a system of law that is used to provide predictability and are templates and frameworks to guide actions and outcomes. The term 'tika' means 'to be right'. Tikanga Māori therefore means the right Māori way of doing things. It is what Māori consider is just and correct. Tikanga Māori includes all of the values, standards, principles or norms that the Māori community subscribe to, to determine the appropriate conduct. Tikanga is therefore comprised of both practice and principle. That is, it includes both the rules (what you should and should not do) as well as the principles that inform the practical operation and manifestation of the rule. The customs or rules of tikanga are acknowledged when they are maintained by the people and are observed in fact."

In addition, Hon Justice Joe Williams of the Supreme Court has described tikanga as "*Law designed for small, kin-based village communities. It is as much concerned with peace and consensus as it is with the level of certainty one would expect of normative directives that are more familiar in a complex non-kin-based community. In a tikanga context, it is the values that matter more than the surface directives. Kin group leaders must carry the village with them in all significant exercises of legal authority. A decision that is unjust according to tikanga values risks being rejected by the community even if it is consistent with a tikanga-based directive.*"

See Williams, Joseph "*Lex Aotearoa: An Heroic Attempt to Map the Maori Dimension in Modern New Zealand law*" (2013) 21 Wai L Rev 2.

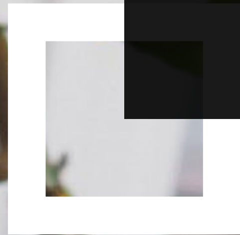
6 *Doney v Adlam* (No 2) [2023] NZHC 363.

7 *Kruger v Nikora* [2023] NZCA 179.

8 *Pact Group v Robinson* [2023] NZEmpC 173; *GF v Comp troller of the New Zealand Customs Service* [2023] NZEmpC 101; *Moke v Raukura Hauora o Tainui Trust* [2023] NZERA Auckland 603; *SFC v YKQ* [2023] NZERA Christchurch 529.

9 *Peter Ellis v R* [2022] NZSC 114 at [22].

An ever-evolving workplace



Changes in the workplace impacting business

Our employment institutions, especially the Employment Court, are driving material change.

Worker status litigation

The gig-economy continues to expand in New Zealand (and globally), and so does litigation over worker status. For this reason, worker status remains front of mind for many workers and organisations (both public and private employers/engagers). The steady flow of worker status litigation is set to continue this year, and we wait to see whether worker status (and any reform) is a priority for the Coalition Government. In the absence of legislative reform, development of our worker status framework will continue to take place before our courts with strong union backing.

There are three notable proceedings that are currently on foot. We describe these below:

2022 saw the Employment Court deliver its second judgment on the status of Uber drivers in New Zealand.[1] In an outcome that differed from the outcome reached by the Employment Court in respect of a different Uber driver in 2020,[2] the Employment Court declared that the Uber drivers involved the 2022 case were employees. In June 2023, the Court of Appeal granted Uber leave to appeal. That matter is expected to be heard by the Court of Appeal this year. Though the outcome of the case will inevitably be fact-specific, the Court of Appeal's judgment may contain further guidance on the application of the statutory test.

Last year, the Employment Court also considered a second worker status case concerning the residents of Gloriavale. It found that the female plaintiffs, who undertook cooking, cleaning, washing and food preparation duties, were employees.[3] Leave to appeal has been sought, which could mean another significant judgment this year.

Finally, the Postal Workers Union of Aotearoa has filed proceedings in the Employment Court on behalf of a small group of NZ Post courier drivers, claiming these drivers are employees who have been misclassified as contractors.[4] There is a long history of courier drivers challenging their employment status, and the decision on this matter is likely to have significance for the industry.

The current statutory test to determine whether a worker is an employee, under section 6 of the Employment Relations Act 2000, requires a determination of the "*real nature of the relationship*" between the parties. Determining the outcome in each case requires an intensely factual assessment of "*all relevant matters*".

Testing jurisdictional boundaries

In 2021, the Supreme Court delivered its judgment in *FMV v TZB*[6]. The Supreme Court confirmed that the Employment Relations Authority's exclusive jurisdiction to make determinations about "*employment relationship problems*" is extensive, diverse, and includes employment-related tort claims, which ought to be brought in the employment jurisdiction rather than in the ordinary courts.

Over time, we expect to see issues that have not previously been brought before the employment institutions being litigated in the specialist jurisdiction.

1 *E Tū Inc v Rasier Operations BV* [2022] NZEmpC 192.
2 *Arachchige v Rasier New Zealand Ltd* [2020] NZEmpC 230.
3 *Pilgrim v Attorney-General* [2023] NZEmpC 105.
4 NZ Post courier drivers launch case arguing they are employees
5 *Webb v Professional Relief Services Ltd* ERA Auckland AA457/10, 22 October 2010; *Cameron v PBT Couriers Ltd* ERA Christchurch CA143/08, 25 September 2008.
6 *FMV v TZB* [2021] NZSC 102.

The Supreme Court emphasised the specialist nature of the employment jurisdiction, and the relational approach of the Employment Relations Act 2000, with the key principle of good faith sitting at the heart of that approach.

Mutual obligation of good faith: The heart of the employment relationship

The Supreme Court's emphasis on the importance of good faith in employment relationships has been echoed in a number of decisions last year from New Zealand's Employment Court.

One judgment emphasised an employer's statutory consultation obligations when proposing to make a decision that will, or is likely to, have an adverse effect on an employee's employment and observed these obligations amplified the core duty of good faith.[7] Another provided a reminder that there is a broad discretion under the Employment Relations Act 2000 to impose penalties for breaches of good faith.[8]

Looking ahead, we expect to see a continued focus on good faith by the Employment Relations Authority and the Employment Court, especially if other aspects of an employee's claim are not strong. This will in conjunction with the increasing emphasis on tikanga in employment relationships (see our further comments in the article "The korero continues: Recognition of tikanga Maori by New Zealand Courts" on page 16.

Non-publication orders: A removal of the presumption of open justice?

Over recent years there has been a steady upwards trend in the number of interim and permanent non-publication orders granted by the Employment Court in respect of one or more parties' identities.

This year we expect a significant judgment from a full bench of four judges of the Employment Court which will examine the legal position on non-publication orders in the employment jurisdiction. The matter was heard in October 2023, and the Employment Court heard submissions from numerous intervenors, including the Privacy Commissioner, the Council of Trade Unions, BusinessNZ, representative bodies from the legal profession, and media organisations. The Court was also assisted by an expert/pūkenga on tikanga. The judgment will provide guidance on whether the current presumption of open justice should remain in place in the specialist employment jurisdiction.

A change in the legal position could result in employment disputes being fought more often behind closed doors. Employers will need to turn their minds to the impact of that on their recruitment processes and on their approach to the resolution of disputes.

Changes under the new Coalition Government

A number of changes to New Zealand's employment laws have recently taken place under the Coalition Government

Most notably, the Fair Pay Agreements Act 2022 has been repealed, dismantling the recently introduced bargaining framework before any fair pay agreements were agreed. And, use of the statutory 90-day trial period has been opened up to all employers, regardless of size. This provides all employers with protection from an unjustified dismissal personal grievance if the employee was dismissed within the first 90 days of employment.

When 90-day trial period legislation was introduced in 2016, a significant amount of litigation followed as the 'rule' created the only exception to an employee's ability to bring an unjustified dismissal claim. As the Government has effectively restored the 90-day trial period to its 2016 state, the case law from that earlier time will apply. That law demands that employers adhere strictly to the legislative requirements. An uptick in trial period litigation can be expected, holding employers to those strict procedural requirements, most likely with an additional good faith lens.

Finally, though no parties campaigned on the matter, we expect some movement changes to the Holidays Act 2003 this year. Once new legislation is passed, we expect litigation will follow as employers and employees work to understand the demands of the new calculations that are expected to be introduced.

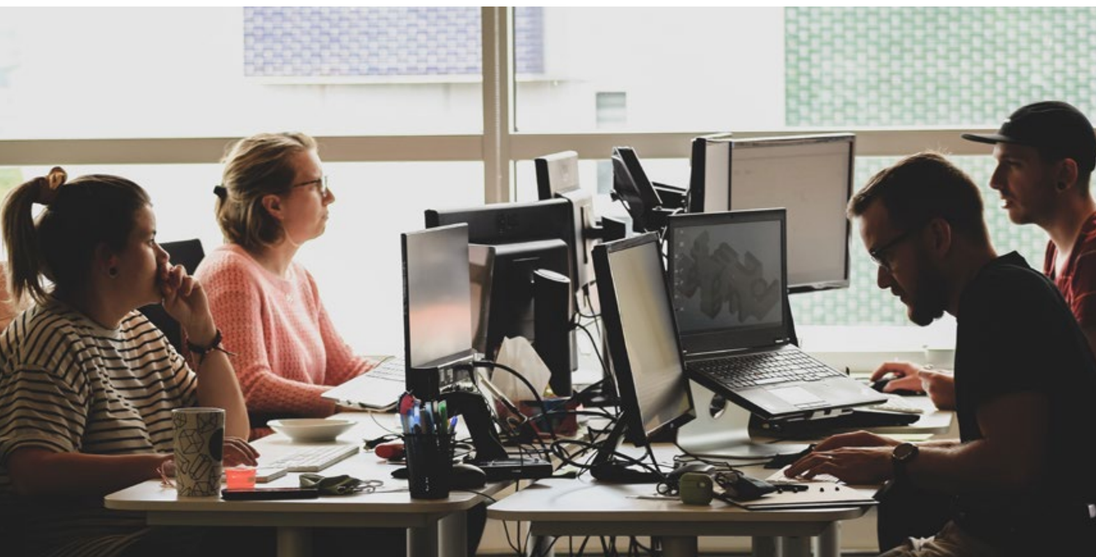
7 *Birthing Centre Limited v Matsas* [2023] NZEmpC 162.
8 *Pyne v Invacare NZ Limited* [2023] NZEmpC 179.

Cyber and generative AI

Cyber risk and litigation:

Some guidelines for directors and boards

Cyber risk is among the top risks facing businesses and other organisations today. New Zealand businesses reported $39.6m in losses from cyber crime in the two years leading up to 2023, and this figure includes only those which reported their losses.[1] Internationally, cyber crime is estimated to cost businesses $10.5 trillion annually by 2025.[2] Furthermore, in addition to losses to cyber criminals and resulting losses to individuals and investors, regulators in New Zealand and abroad are increasingly taking a close interest in what regulated firms are doing to manage cybersecurity risks.



Increased cyber crime results in increased litigation. Claims are made against companies that are victims of cyberattacks that result in private and personal information of their customers and others being released. Claims are made upon insurers when losses are suffered. Remedies are sought from banks and other financial institutions that do not prevent customers' losses resulting from cyber crime. Regulators are increasingly focusing upon the adequacy or regulated entities' cyber protections and the steps being taken by their boards.

Recently, the personal information of 9.7 million Medibank customers was stolen and posted online after its insurer declined to pay a ransom demand. This has resulted in two class actions in the Federal Court of Australia and a proceeding on behalf of the shareholders in the Victorian Supreme Court.

In New Zealand, the Latitude cyberattack in March last year exposed the personal records of 14 million customers, including a million New Zealand driver's license numbers and 40,000 passport records. In response, the New Zealand Privacy Commissioner and the Australian Information Commissioner commenced a joint privacy investigation, a $1 million lawsuit has also been filed by one of the customers affected and registrations are open for a potential class action against Latitude.

Company boards should take note. The World Economic Forum has expressed a view that boards need stronger foundations to govern cyber risks effectively.[3] In an Institute of Directors / ASB Bank survey, just 54% of directors reported that their boards regularly discuss cyber risk and are confident that their organisations have the capacity to respond to a cyberattack or incident.[4]

In this article, we provide key considerations for how directors and boards might mitigate cybersecurity risks and respond to a cyber incident if one occurs.

1 New Zealand Computer Emergency Response Team, Cyber Security Insights (2023)
2 Cybersecurity Ventures, 2021 report: cybersecurity in the c-suite (2021)
3 https://www.weforum.org/publications/principles-for-board-governance-of-cyber-risk/
4 Institute of Directors/ ASB Director Sentiment Survey Report 2022

Managing cyber risks

The Australian Securities and Investments Commission (ASIC) has set out guidelines for good practice in cyber resilience[5] and has said that good cybersecurity strategy and governance are characterised by board ownership and responsive and agile governance models. The Institute of Directors New Zealand has also published a 'practical guide' to cyber risk.[6] In light of these materials and our experience, we set out below some key tips on managing cybersecurity risks.

1. Establish an enterprise-wide cyber risk management framework:

Boards have a responsibility to hold management to account in establishing a fully integrated organisational approach to cybersecurity. Organisations should approach cybersecurity as an enterprise-wide risk, rather than treating it only as an IT issue. A cybersecurity strategy should outline a comprehensive approach to risk management, incident response, and recovery. The World Economic Forum's Principles of board governance of cyber risk is a useful reference for developing a cybersecurity strategy.

2. Give cybersecurity regular attention on the agenda and continue to build cyber competency:

While directors do not need to be cyber experts, they need a sufficient level of understanding to stay on top of key risks and issues. They should consult external expertise where appropriate. It is helpful to ensure that there is cybersecurity expertise at senior management levels and that senior management updates the board on any key changes to cyber vulnerabilities or the wider cyber risk environment. It is helpful to refer to the Institute of Directors guidance on reporting cybersecurity to boards on how to improve cybersecurity reporting.

3. Understand the legal environment:

It is critical that directors understand their legal responsibilities and the implications of cyber risk relevant to their organisation and keep abreast of changing regulatory expectations. A helpful resource is our recent cover to cover article on recent regulatory developments in this area. Regulators such as the Financial Markets Authority and the Privacy Commissioner, as well as insurers, may require notification and/or investigation of cyber and privacy breach incidents.

4. Identify, categorise and address the risks:

Management should identify which cyber risks to avoid, accept, mitigate or transfer through insurance. They may then formulate specific plans associated with each approach. It is helpful to refer to CERT NZ's 11 top tips for cybersecurity for practical guidance on managing cyber risks.

5. Improve long term cyber risk management:

In the long run, organisational changes to improve cybersecurity processes are likely to pay for themselves. Directors should consider:

- **Regular reviews and assurance:** Conduct regular reviews of cybersecurity strategies and security audits to identify vulnerabilities and assess the potential impact of a cyberattack. Results should be measured against success criteria such as time to detection, speed of response and recovery process.
- **Strong cultural focus and training:** For most organisations, the main point of cyber weakness is human frailty. Effective cyber resilience requires a strong 'cultural' focus driven by the board and reflected in organisation-wide programmes for staff awareness, education and random testing of staff and third parties to assess cyber-awareness.
- **Invest in cybersecurity infrastructure:** Implement robust cybersecurity measures, including firewalls, encryption, intrusion detection systems, and secure backup solutions, and keep them all up to date.
- **Manage third-party risks:** Steps include conducting due diligence (such as obtaining independent security attestation reports and certifications), and using contract terms to improve transparency and mitigate fourth-party risk, for example, by requiring suppliers to notify the organisation if their subcontractors or vendors experience a cybersecurity event.

6. Ensure a comprehensive cyber and data breach response plan is in place:

In the event of a cyber breach, an assessment and remediation of the breach will likely be most effective and credible in the eyes of stakeholders, such as the Privacy Commissioner and affected individuals, if undertaken within the context of a tested data breach response plan. The New Zealand Privacy Commissioner and the Office of the Australian Information Commissioner have set out four key steps in dealing with a privacy breach: contain, assess, notify and prevent / review.

5 Cyber resilience good practices | ASIC.
6 Institute of Directors New Zealand, Cyber risk: a practical guide 2023

Responding to a cyber incident

In the event of a cyber incident, it is important to be prepared. As the Institute of Directors has observed, organisations that have not planned for an incident tend to perform badly; they tend to panic and waste time and energy working out their approach, while the attacker continues to disrupt services or access confidential data.[7]

We set out some key steps and considerations that could form part of a cyber response plan.

Identify and contain

Identify and contain the breach to prevent further data loss. This may involve taking affected systems offline or restricting access.

Assess the impact

Determine what data has been compromised, how many individuals are affected, and what the potential consequences could be. This will help in formulating a response.

Notify relevant parties

If the breach meets the threshold of 'serious harm' under the Privacy Act 2020, organisations are required to notify the Privacy Commissioner and affected individuals "as soon as reasonably practicable."

See our podcast on the various factors that should be considered when assessing the 'serious harm' threshold, and how organisations should interpret the requirement to notify "as soon as reasonably practicable".

Investigate and remediate

Investigate how the breach occurred and take steps to fix those vulnerabilities and prevent future breaches.

Keep proper records

Keep records of the assessment of the breach, response, and any remediation. This is particularly important if an organisation is called upon to justify not reporting a breach because it has judged it unlikely to cause serious harm. Note however that these records are likely to be discoverable in any litigation, so ensure that they are prepared with this in mind, avoiding any unhelpful statements or critical comments.

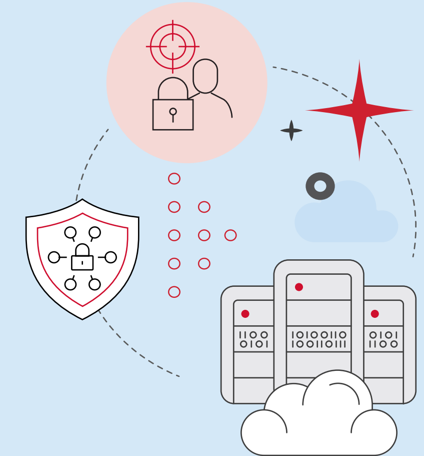
Consider privilege issues

Legally privileged documents may be withheld in litigation or during a regulatory investigation, but it is critical that the right steps are taken before and during a cyber incident to maintain and avoid inadvertently waiving privilege. Communications will typically be privileged where they take place with a legal advisor for the purpose of giving or receiving legal services. Communications may also be privileged where they are made for the dominant purpose of preparing for an anticipated legal proceeding. However, communications made for other purposes, or communications that are not intended to be confidential, will not be privileged.

In the event of a cyber incident, communications and documents with the following purposes are at an increased risk of requiring disclosure in litigation:

- investigating the cause of a cyber incident;
- informing stakeholders about a cyber incident; and
- discussing existing or new cybersecurity processes.

The recent Optus class action proceeding highlights this issue, which we discuss over the page.



7 Institute of Directors, Cyber risk: a practical guide, 2023 edition

Maintaining privilege when responding to a cyber incident: lessons from the Optus class action

When a cyber incident occurs, the affected organisation may wish to commission an investigation (whether internal or external) into the incident. This can be risky, as the resulting report may be helpful to litigants who bring proceedings against the organisation and/or its directors. The report may identify what was done wrong and may criticise the organisation.

A recent Federal Court of Australia judgment underscores the importance of proper privilege protocols before an incident occurs. Belatedly setting up privilege protocols and processes will not retrospectively confer legal privilege upon an investigation report. The purposes of preparing the report, and evidence which demonstrate those purposes, are critical when a privilege claim is challenged.

In September 2022, Optus, the Australian telecommunications service provider, suffered a data breach that affected the personal information of up to 10 million customers. Optus engaged external solicitors to provide legal advice and instructed Deloitte to conduct a forensic review of the attack and complete a report.

Following these events, a class action claim was brought against Optus in the Federal Court of Australia claiming that that it failed to protect or take reasonable steps to protect customers' personal information. The Deloitte forensic review contained information relevant to the claim, but Optus refused to discover it and similar documents, claiming that they were subject to legal professional privilege.

The Federal Court found that the report was not privileged, despite Optus claiming that its dominant purpose was for the purpose of legal advice or litigation. The Judge placed considerable weight on a press release issued by Optus shortly after the data breach[8] which included the following comment[9]:

"this review will help ensure we understand how it occurred and how we can prevent it from occurring again. It will help inform the response to the incident for Optus. This may also help others in the private and public sector where sensitive data is held and risk of cyberattack exists"

The Court held that the Deloitte report was not privileged because it was prepared for a number of purposes, not for the dominant or overriding purpose of legal advice or litigation. While one of the purposes of the report was to provide legal advice for the purpose of litigation or regulatory proceedings, other purposes included identifying the circumstances and root causes of the cyberattack, rectification, and reviewing Optus' management of cyber risk in relation to its policies and processes.

There are differences in the law governing legal advice privilege in New Zealand and Australia. Unlike in Australia, New Zealand's statutory definition of legal advice privilege makes no mention of the need for a dominant purpose, although the statutory definition of litigation privilege does. It is possible that the New Zealand courts may require only that legal advice was only one of the purposes for which a report was created, but this does not appear to have been settled, so it would be prudent for organisations to assume that reports will only be protected where their primary purpose was to inform legal advice.

Another difference is that in Australia, a third-party expert report may be protected by legal advice privilege if it was produced for the primary purpose of enabling lawyers to provide legal advice. In New Zealand, the relevant provision of the Evidence Act describes legal advice privilege only with respect to documents passing between clients and their lawyers, not third parties such as experts. It is possible that legal advice privilege may attach on the basis that the third parties are agents of the client, but that will depend on the facts of each case. Litigation privilege is different, as privilege will attach to documents prepared by third parties where the dominant purpose was to enable the client to instruct lawyers, so where litigation is reasonably contemplated that may be a more effective method of protecting a report. Ensuring that a report is protected by legal privilege is not straightforward and should be considered carefully from the outset.

8 Robertson v Singtel Optus Pty Ltd [2023] FCA 1392.

9 Optus, Optus commissions independent external review of cyber attack

Best practice steps for protecting legal privilege:

Establish and follow legal privilege protocols:

Establishing proper privilege and confidentiality protocols prevents inadvertent waivers of privilege in a stressful and time-sensitive scenario such as a cyber breach.

Seek legal advice early:

Understanding disclosure and reporting obligations following a cyber incident is crucial. Protecting documents with privilege may also be important. Promptly consulting a legal adviser will assist in navigating these priorities.

Be clear when stating the purposes of inquiries:

To claim privilege in respect of documents or communications created as part of an inquiry into a cyber incident, in summary, the document or communication must be created by the client for the purpose of legal advice or by the client or a third party for the dominant purpose of preparing for a legal proceeding. To assist in successfully asserting privilege over these materials, the legal purpose must be unambiguously stated and supported by contemporaneous evidence. It is also important to ensure consistency in the messaging of internal and external communications, which Optus did not do effectively.

Exercise particular care with multi-purpose reports and documents:

Where a report is commissioned for a number of purposes, a privilege claim is at risk of challenge. Documents prepared by in-house counsel may be more prone to challenge than if prepared by external legal advisers, as in-house staff more often provide non-legal business and strategic advice which does not attract privilege.

Final remarks

Cyber risks increasingly result in litigation. We see this trend continuing. Organisations should respond by preparing to counter cyber risks and have a well-developed plan for responding to a cyber event that provides not only for the IT response but also for the legal risk that follows.

Navigating the legal minefield:

Generative AI and its implications for businesses and directors

Generative AI, a subset of artificial intelligence that relies on large quantities of data, neural network architecture, and complex algorithms to produce original content, is rapidly transforming the business landscape.

From content creation to product design, customer service and marketing, generative AI is proving to be a game changer. McKinsey's latest research estimates that generative AI's impact on productivity could add $2.6 trillion to $4.4 trillion annually in value to the global economy.[1]

However, like any powerful tool, generative AI comes with its own set of risks and challenges. Similarly, if the data set being used is erroneous, or restricted in any way, that can lead to inaccurate outputs. AI models can 'hallucinate' (i.e. create and rely on false data). Further, AI models often make decisions in a 'black box', meaning there may be no way for users to understand exactly how the AI has made its decisions (and in a litigation context, creating issues around discovery obligations and proof).

In this article, we set out some precautions that businesses and directors should take to minimise the legal risks of using generative AI, with a focus on privacy and copyright risks.

Privacy

The use of AI tools present specific challenges for privacy. This is particularly the case for generative AI, which rely on large quantities of data. AI enables new ways to gather and combine personal information, and can make it harder to see, understand, and explain how personal information is used. It is therefore important to understand the privacy risks of using AI before implementing it. This requires some understanding of how the AI tool works, such as knowing what data sources they were trained on, and how relevant and reliable these sources are for your purposes.

In New Zealand, there are currently no laws or regulation specific to the use of AI. The Privacy Act 2020 applies to the use of AI. On 21 September 2023, the Privacy Commissioner issued new guidance on how the Information Privacy Principles (IPPs) can be applied to the use of AI, which builds off the Commissioner's initial set of expectations (published in May 2023).

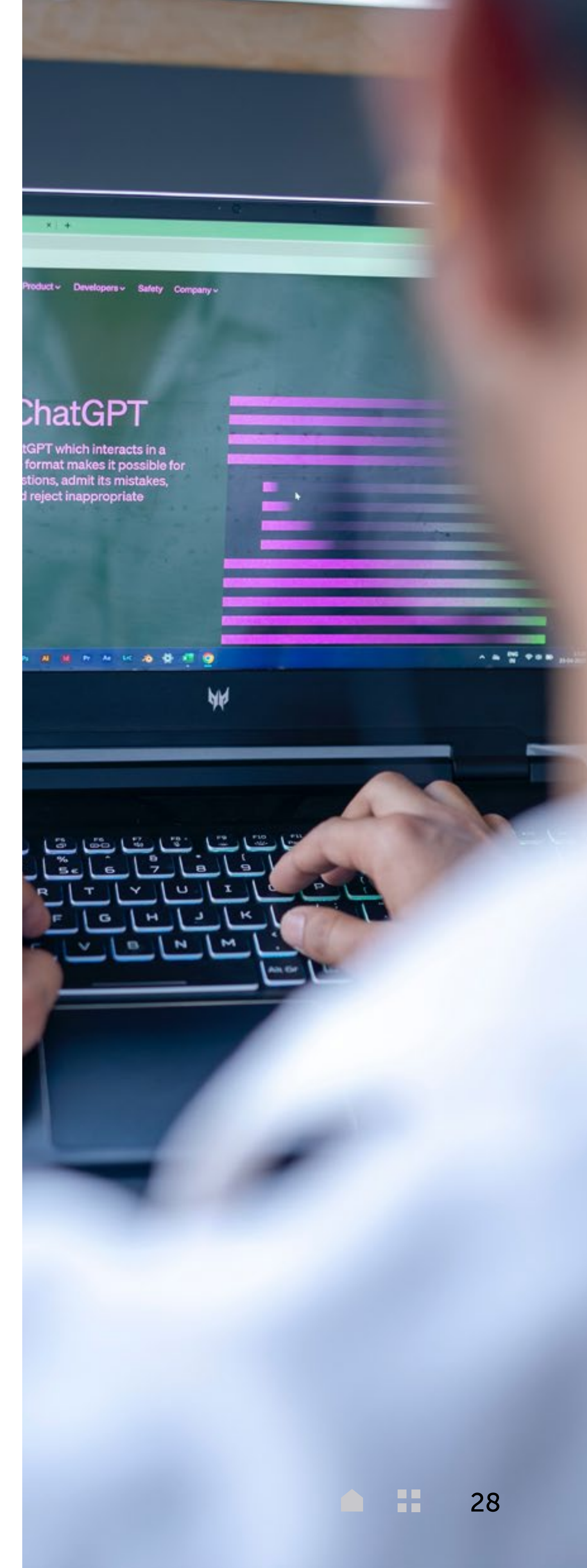
We set out a short summary of the guidance below.

- IPPs 1-4 cover why and how personal information can be collected. This requires an understanding of the training data and processes used to develop an AI tool.
  - If you have already collected personal information and want to feed it into the AI, think about the purpose for which you originally collected the information, and whether feeding the information into AI is directly related to that purpose (IPP1).
  - In general, agencies must get personal information directly from the person it is about (IPP2) and must be transparent about the information being collected and how it will be used (IPP3). While there are some exceptions to the normal collection principles, such as the exception for "publicly available" information, it may be risky to rely on these exceptions without a good understanding of the training data and processes used for an AI tool. For example, training data scraped from the internet may include sources which require a login to access, such as social media profiles, which may not be publicly available and outside the expectations people have on how this information would be used.
  - Ensure that input and training data are collected in a way that is lawful and fair (IPP4), and relevant individuals know how and why their data is being used.

1 https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier#key-insights

- Proactively consider how to manage security risks and unauthorised access to personal information, such as taking cybersecurity measures (IPP5). AI tools enable new ways to access and use information, and this creates new security risks. Some AI tools can leak sensitive information. Consider setting up privacy breach response plans to ensure you can identify, contain, assess and respond to privacy breaches quickly. For more information on how to manage a data breach, see our podcast on this topic.
- Develop procedures for how your organisation will respond to requests from individuals to access and correct their personal information (IPP6 and IPP7). Before purchasing an AI tool, consider whether you are able to practically access personal information about a person if they ask for it, and correct any personal information if required.
- Be aware of the limitations of the tool, including gaps, biases and 'hallucinations', and take steps to ensure accuracy (IPP8). This includes ensuring the training data is relevant and reliable, and putting checks in place (such as human review) to ensure accuracy of output.
- Clearly identify the purpose(s) for collecting personal information, and limit its use and disclosure to those purposes or a directly related purpose (IPPs 10 and 11). If you want to use personal information to train an AI tool, make sure that is clear at the time you collect the information. If you are sharing personal information with third-party suppliers, ensure they are not using the information for training AI tools unless that is why the information was collected. In supplier contracts and customer communications, set clear expectations about how personal information will be used and kept secure.
- The Privacy Commissioner recommends conducting a privacy impact assessment (PIA) before using any AI tool, and seek feedback from impacted groups.

As a general tip, if purchasing an off-the-shelf AI tool, we suggest asking the provider for documentation of the sources and collection of input data, as well as assurances (or a warranty) that individuals whose data is inputted into the AI tool have consented to any collection and use of their personal information. Carefully review the terms and conditions for how (and what) information is retained and disclosed. In general, avoid inputting personal or confidential information into the tool, unless you are confident that the information is not retained and disclosed by the tool. If in doubt, strip input data of any information that enables re-identification and anonymise any data that is shared.



Copyright

While the use of generative AI can create various intellectual property issues, particular issues arise in relation to copyright. Whilst the usual base principles in assessing copyright (including subsistence, originality and infringement) are all relevant, the use of generative AI raises new, untested questions, including in respect of these otherwise relatively settled areas. These include whether copyright subsists in AI-generated content, who the author is, and the scope of protection. The legal position will vary between jurisdictions.

AI training data

Where the input data is a copyright work, making an unauthorised copy of that work could amount to an infringement. Where AI input data does infringe copyright, a third party that uses this data to generate output also risks infringement if the output is considered a copy of, or a copy of a substantial part of input data.[2]

While untested in New Zealand, legal action is being taken against AI providers in other jurisdictions for IP infringement. Some examples of this are set out below.

- In early 2023, Getty sought an injunction to prevent the artificial intelligence company, Stability AI, from selling its AI image-generation system, in the United Kingdom and United States. This followed the creation of an image by Stability AI which clearly showed a 'Getty Images' watermark. Getty has made various claims against Stability AI in both the UK and the US, including copyright infringement and trademark infringement. The claims relate to both input and output of Stability AI. These cases, once they eventually reach trial, will address previously untested issues about the legal implications of using others' works to train AI.
- In September 2023, several authors in the United States (including former attorney John Grisham) initiated legal action against OpenAI alleging infringement of their original works.
- Also in September 2023, the New York Times filed legal proceedings against OpenAI for infringing authors' copyright.

AI outputs

The New Zealand Copyright Act 1994 (the Copyright Act) currently allows computer-generated works to be protected by copyright.[3] The Act provides that the owner of the copyright is the author of the work, being the person who "*made the arrangements necessary*" for the creation of the work.[4]

However, the current position in many overseas jurisdictions, including Australia and the United States, is that creative works require a human author to attract copyright. The Copyright Act is under review, and it is unclear whether the current position will change but we expect it unlikely that the permissive regime in New Zealand would be reduced in scope. To attract copyright under the Copyright Act, the work must be original.[5] The extent of originality depends on how much skill, labour, and effort the author has put into creating it.[6] While the threshold for originality is low,[7] it is unclear whether some human skill and effort is required for the AI-generated work to attract copyright, and if so, the level of effort required.

Another related question is who owns the copyright, being who "made the arrangements necessary" for the creation of the work. If a business develops and uses its own AI tool (including using internal training data), the business is likely to be the owner of the AI-generated content provided the usual parameters for copyright subsistence are met (and subject to any third party rights). However, if a business uses an external AI tool, it is unclear whether ownership of the output belongs to the business, the AI provider, another contributor of the tool, or is shared between different parties. This question may depend on the extent to which the AI output is amended from the original 'prompts', whether prompts amount to copyright works, and the extent to which the eventual output is amended from the AI output. All these factors are also able to be varied by contractual provisions (including terms and conditions), which will be important to assessing rights.

Who owns the copyright of AI-generated content and any third party rights in it impacts the scope of permitted use and whether a business can monetise the content (and any associated infringement risk). Whilst AI tools such as OpenAI grant a licence for use, input data and outputs are also subject to contract terms, so exclusivity is likely to be lost. In addition, there may still be a risk of infringement. It also presents issues as to whether the business can enforce copyright in the goods or services that incorporate the content, such as where similar content may appear in a competitor's product or marketing material.

2 Copyright Act 1994, s 29.

3 The term "computer-generated" is defined in section 2 as "the work is generated by computer in circumstances such that there is no human author of the work."

4 Copyright Act 1994, s 5(2)(a).

5 Copyright Act 1994, s 14(1) and (2).

6 *Wham-O MFG Co v Lincoln Industries* [1984] 1 NZLR 641 (CA) at 665.

7 *Henkel KGaA v Holdfast New Zealand Ltd* [2007] 1 NZLR 577 (SC) at [38].

Numerous platforms (including Adobe, Google and Microsoft) now offer indemnities for the end users of their generative AI programmes against any third-party copyright infringement claim, but strict requirements and indemnities are imposed and this is unlikely to provide complete protection.

Some precautions to take to minimise IP risks when using generative AI:

- If purchasing an external AI tool, check whether the AI provider offers a robust indemnity for any infringement of IP from the use of the tool and requirements to ensure the indemnity applies.
- The terms of use of many AI providers assign ownership of inputs and outputs, or grant a use-only a licence to its users. This is likely to mean your input data is available to others to use, as is the output. However, as noted above, it is prudent to ask for the documentation of the sources of input data. If the AI provider does not own the data, ensure that the provider has obtained relevant consents and/or licences from any external parties who may own the data. Ensure that any use of the AI tool does not infringe upon those consents and/or licence conditions.
- Avoid input of data that is confidential, is likely to be used for a patented invention (as the required confidentiality may be lost) or strategically important to the business for these reasons;
  - Try to identify if use of AI generated content means you are inadvertently using open-source software as the open-source licence terms may be inappropriate, with similar issues for materials that are creative commons.
  - If in doubt, use internally generated and owned data to train models. Keep records of all inputs that go into the AI tool, such as prompts, which can help to show that the business "made the arrangements necessary" to create the output. However, be aware that a limited dataset could introduce bias (or other issues) into the model.
  - Be aware that you may be unable to prevent others from using a similar AI output, if you are not modifying the AI generated output.

Each organisation's IP policy will differ, and there is no one-size-fits-all approach to ensuring your IP policy mitigates against risks of using generative AI. It is important to obtain specialist IP advice in respect of such policies, and also alongside litigation advice should matters become contentious.

Implications for organisations, employers and directors

Under the Companies Act, a director must exercise the care, diligence and skill that a reasonable director would exercise in the same circumstances.[8] With the increasing use of generative AI, an emerging and untested question is whether directors have an obligation to inform themselves of the use of AI by their organisation, and to ensure that AI is used in appropriate circumstances. This raises further questions about what those circumstances might be. Where AI is informing or assisting in the decisions of directors, this raises the further questions regarding of the responsibility of directors for the outputs of those decisions.

While this question may be clarified by the Courts and/or the legislature over time, it is important that directors and businesses take steps to mitigate against the legal risks of using (or not using) generative AI. Importantly, businesses should ensure that there are clear employee policies in place setting out where generative AI may be used and that privacy statements set clear expectations for use. We recommend being clear and upfront to customers about any use of generative AI, including how you are managing the associated privacy, IP, and other risks.

Organisations should also keep on top of emerging regulation in this space. The European Union, United States and Australia are progressing with AI-specific regulation, and New Zealand will likely follow suit in the future.

8 Companies Act 1994, s 137.

Health and safety

Health and safety prosecutions:

The outlook post-Whakaari White Island

On 31 October 2023, Whakaari Management Limited (WML) was convicted in the District Court in relation to a charge filed by WorkSafe New Zealand (WorkSafe) under s 37 of the Health and Safety at Work Act 2015 (HSW Act). This decision marked the culmination of the liability stage of one of the most significant health and safety proceedings in New Zealand's history.[1]

When WorkSafe began its investigation of those involved in tourism to, or connected with, Whakaari | White Island (Whakaari), 13 defendants faced charges. However, since the proceedings began in 2020, six of the defendants pleaded guilty, and a further six had their charges dismissed (either prior to or during the trial), leaving WML the sole remaining defendant at the end of the trial.

The overall outcome of the proceedings – and, in particular, the number of charges dismissed – will be disappointing for those affected by what happened at Whakaari. We also consider the outcome of the proceedings is likely to cause WorkSafe to reflect upon how it investigates health and safety incidents and makes decisions on charges going forward.

Of note in the Whakaari proceedings is that WML defended charges brought by WorkSafe under ss 36(2) and 37(1) of the HSW Act and succeeded in having the charge under s 36 dismissed.

It is noteworthy that Judge Thomas' interpretation of s 36(2) followed orthodox statutory interpretation which accounted for:

- the language and structure of s 36 (and the HSW Act as a whole);
- the indicators of purpose within the HSW Act; and
- the relevant legislative history.

Judge Thomas' approach to interpreting the HSW Act is something to be borne in mind in any future litigation in terms of the approach the courts might take to interpreting the Act.

Similarly, the directors of WML had their charges dismissed after WorkSafe called its witnesses and closed its case. The charges against the directors of WML were dismissed on the basis that Judge Thomas did not consider he could reasonably convict any of them on the evidence brought by WorkSafe. WorkSafe's evidence only reflected the action or inaction of the directors as a group, whereas the charges against each director had to be proved individually.

1. We have discussed the prosecutions in greater detail in our previous alert - Culmination of liability stage of Whakaari White Island proceedings.

Judge Thomas set clear expectations as to what WorkSafe should ask directors, identifying the following questions as essential to the assessment of individual due diligence:

- Did they as a board agree that all three of them should have the responsibility for looking into whether and what expert advice WML should take?
- Did they agree that one in particular was more able to perform that role than the others, or two of them?
- Did they argue or disagree about how much should be done?
- Was anyone outvoted on that?
- Did that person do all that they could but was simply outnumbered?

WorkSafe's failure to obtain convictions against a number of defendants in the Whakaari proceedings may result in more defended hearings as other defendants reconsider the relatively common approach in New Zealand of entering early guilty pleas and seeking to mitigate adverse outcomes at sentencing. Indeed, it is not common for defendants to defend a charge during a health and safety prosecution (and therefore for WorkSafe's case to be tested). This is often because of the commercial and other sentencing discount incentives that defendants have to plead guilty at an early stage of a proceeding.

The Whakaari outcome may also cause WorkSafe to reflect harder on what matters to take to trial and whether additional rigor should be applied to testing whether the evidence developed during investigations is sufficient to make out any charges being contemplated.

We expect that prospective defendants to a WorkSafe prosecution will take some confidence from the dismissal of charges in the Whakaari proceedings and will be more likely to either:

- test the appropriateness of charges brought by WorkSafe at the outset;
- seek the dismissal of charges brought by WorkSafe; or
- defend the charges during a trial.

In response to the dismissal of charges against various defendants in the Whakaari proceedings, a campaign has been established, by two people who lost loved ones during the Pike River Mine disaster, to introduce corporate manslaughter legislation in New Zealand. The campaign follows on from the similar "Not One More" campaign launched early in 2023 by the New Zealand Council of Trade Unions (NZCTU), the purpose of which was to lobby for legislation that would amend the legal definition of homicide to include killing by a "non-natural person". NZCTU proposed that this would involve:

- expanding the Crimes Act's definition of culpable homicide to include death resulting from health and safety breaches; and
- importing the concept of PCBU liability for corporations from the Health and Safety at Work Act 2015 (the HSWA) into the Crimes Act's "Interpretation" section.

We have not seen any clear indication that New Zealand is looking to adopt a corporate manslaughter offence. We note that before the 2023 General Election, New Zealand First indicated it was taking the proposal made in the more recent campaign seriously. The National Party thanked the pair behind the latest campaign for voicing their concerns.

Outside the Whakaari proceedings, 2023 also saw record fines imposed in cases involving fatalities, with an unprecedented $502,500 fine imposed on AFFCO New Zealand Ltd after the death of a worker in an abattoir. Other significant fines imposed in 2023 include $440,000 against NZSki Limited, and $270,000 against sister companies ABC Aluminium Limited and Ultimate Design and Renovation Limited. It is noteworthy that the higher fines for NZSki and AFFCO were imposed in cases where the PCBU had been put on notice of the relevant risks and hazards but failed to take sufficient action to eliminate or minimise them.

Steve Haszard has been appointed as WorkSafe's new Chief Executive. This change in leadership comes at a time when WorkSafe is facing significant budgetary pressures. These pressures have seen WorkSafe introduce a 'sinking lid' on jobs, with cost-cutting measures forecast to continue in 2024. In order to achieve a more sustainable funding model, WorkSafe has announced a new organisational structure that will reduce costs by reducing the overall number of roles within WorkSafe. However, the cost-cutting measures are not intended to impact on WorkSafe's inspectorial and investigation capabilities; on the contrary, WorkSafe has announced its intention to increase its staffing numbers in these areas over time. This decision may be designed to reverse a recent trend where, over the past several years, there has been a steady decline in the number of investigations conducted each year, from 360 in 2016 to only 100 in 2023, despite WorkSafe reporting a stable number of work-related fatalities and a rising number of workplace injuries over the same period.

Our Litigation and Dispute Resolution team

Our national Litigation and Dispute Resolution team has an outstanding track record for resolving the most challenging disputes, and providing clients with practical advice on the law and litigation strategies that enhance their prospects of success.

Ranked Tier 1 by The Legal 500 Asia-Pacific, we have some of New Zealand's most experienced and proactive litigators.

Our team leads the way in providing legal advice on a wide range of disputes in the commercial, insurance, insolvency, financial, consumer, regulatory, energy and environmental, public law and IT spaces, as well as in health and safety matters, litigation funding and class actions, and cross-border disputes.

Our aim is to help our clients avoid disputes wherever possible, which is why our team offers commercially astute advice to resolve matters at an early stage and guide you through mediation and arbitration if that is the right option. We are also right at home at all levels of the court system including the High Court, Court of Appeal and Supreme Court.

Legal advice across borders and quick access to courts is no problem either, thanks to our international network through the MinterEllison Legal Group.

MinterEllisonRuddWatts' is extremely commercial, very client focused and understands the client's goals"

Chambers Asia-Pacific 2023

Speak to our experts

MinterEllisonRuddWatts.

We are experts in risk and our full service, top tier Litigation and Dispute Resolution team is ready to assist you with litigation, mediation, arbitration as well as risk management at the executive and board level.

Gillian Service
Division Leader and Partner

+64 9 353 9817
+64 21 366 760
gillian.service@minterellison.co.nz

Richard Gordon
Division Leader and Partner

+64 4 498 5006
+64 27 705 5113
richard.gordon@minterellison.co.nz

Briony Davies
Partner

+64 4 498 5134
+64 27 444 9736
briony.davies@minterellison.co.nz

Nick Frith
Partner

+64 9 353 9718
+64 21 920292
nick.frith@minterellison.co.nz

Sean Gollin
Partner

+64 9 353 9814
+64 21 610 867
sean.gollin@minterellison.co.nz

June Hardacre
Partner

+64 9 353 9723
+64 21 105 9616
june.hardacre@minterellison.co.nz

Andrew Horne
Partner

+64 9 353 9903
+64 21 2451 545
andrew.horne@minterellison.co.nz

Aaron Lloyd
Partner

+64 9 353 9971
+64 21 532 000
aaron.lloyd@minterellison.co.nz

Megan Richards
Partner

+64 4 498 5023
+64 21 676 430
megan.richards@minterellison.co.nz

Stacey Shortall
Partner

+64 4 498 5118
+64 21 246 3116
stacey.shortall@minterellison.co.nz

Jane Standage
Partner

+64 9 353 9754
+64 21 411 728
jane.standage@minterellison.co.nz

REFLECT

PROTECT

ADVANCE

minterellison.co.nz

MinterEllisonRuddWatts.