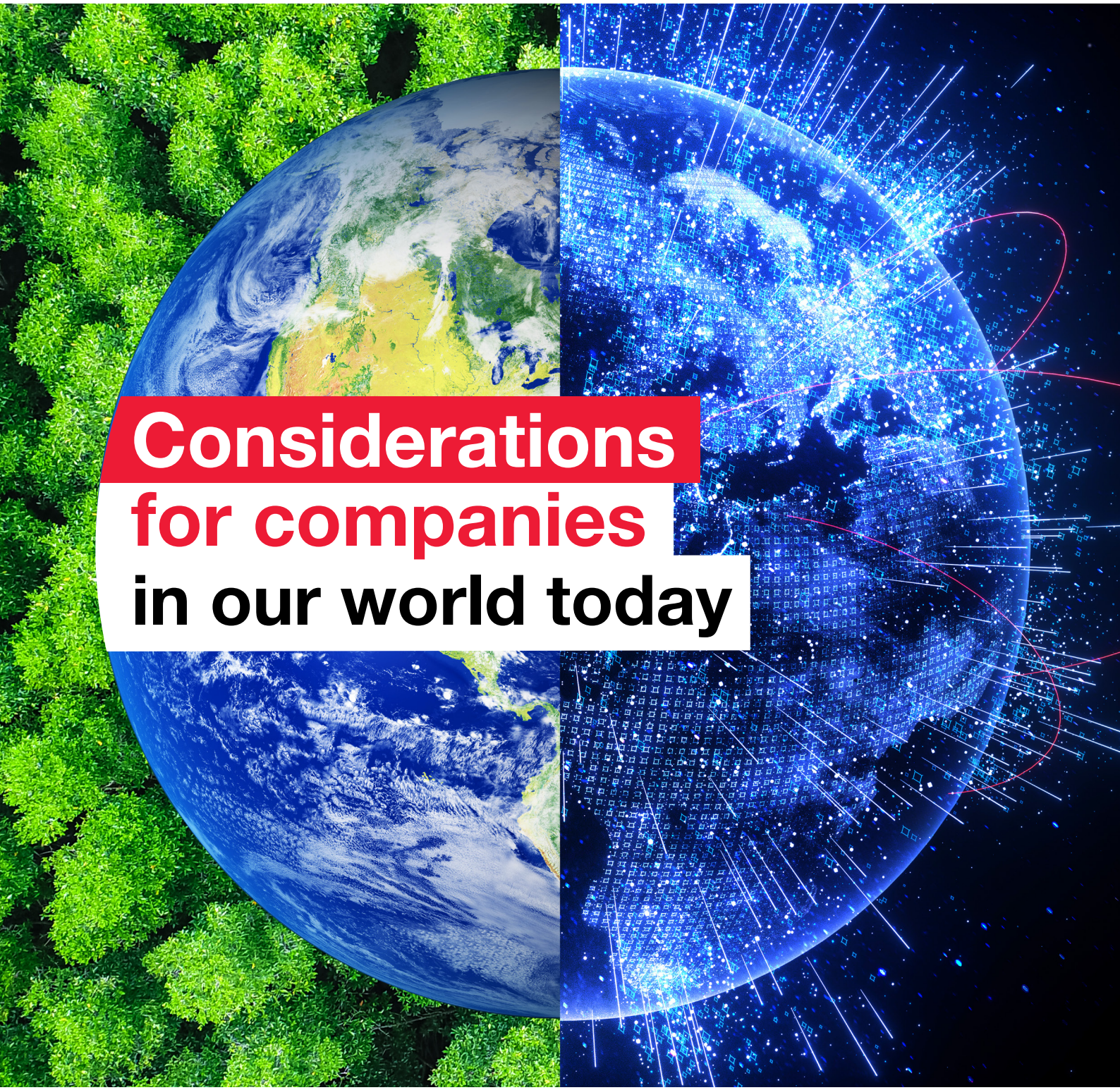
# Next.

## Business, Risk and the Environment today

KING&WOOD MALLESONS
金杜律师事务所

Issue 3 • October 2021



# Considerations for companies in our world today

- **Green New Deals** – What does a sustainable recovery look like?
- Climate disclosures **heat up**
- **Cybersecurity** class actions

# Contributors

**Claire Rogers** appointment as Head of Climate Change Strategy at KWM is supported by her impressive resume in the renewables sector, with a wide range of project financing experience acting for sponsors and financiers in relation to major renewable energies developments and acquisitions. With a unique practice in the Australian market, Claire advises sponsors and lenders on highly complex projects including cutting edge renewable energy transactions and low emissions technologies. Claire's clients benefit from her extensive experience, strategic approach and strong network and reputation with financiers, sponsors and government.

**Renae Lattey** is the Managing Partner, Clients and Mergers & Acquisitions at King & Wood Mallesons Australia and is responsible for the development and implementation of the firm's client and sector strategy. Renae is passionate about transforming the client experience, creating a consistent approach to building strong and deep client relationships, and collaboration between external providers and in-house teams to drive automation, improve process efficiency and adopt new ways of working together as market forces continue to shift industry demands. She is also the firm's TMET sector leader and is well-recognised for her expertise in telecommunications, continuing to provide advice on a wide range of regulatory and commercial issues, telecommunications law and major transactions in Australia and across the South Pacific.

**Mark Beaufoy** is a specialist environmental lawyer with more than 20 years' experience. Mark acts for business and various levels of government advising on environmental regulatory compliance (in particular in relation to contamination, waste, pollution and hazardous substances) and responding to regulatory action. Mark acts for clients across the Industrial & Consumer, Energy & Resources, Agriculture, Infrastructure and Real Estate sectors. Mark has represented many clients in response to regulatory investigations and legal proceedings (including remedial notices, enforceable undertakings and prosecutions) by both state EPAs and federal environmental regulators. Mark regularly presents at industry conferences including Clean Up and EcoForum and was recently awarded the recognition of the 2019 Lawyer of the Year in Contaminated Land and Groundwater by ALGA. Mark is also a sessional lecturer in environmental and planning law at Monash University.

**Meredith Paynter** is a partner in the Mergers & Acquisitions team with more than 25 years' experience advising leading Australian and multinational clients on major M&A transactions. Meredith is a trusted adviser to her clients, acting on their most significant, complex and sensitive transactions. Meredith provides counsel on a range of issues in order to support her clients to successfully implement their strategies and achieve their objectives. Meredith regularly advises clients on corporate governance, continuous disclosure and securities law issues and ASX listing rule matters. Meredith has been the co-author of KWM's "Directions" reports, which reports on current issues and challenges facing Australian directors and boards, for over a decade.

**Michael Swinson** is a partner in the Tech / IP team. Michael specialises in commercial transactions involving technology, data assets and intellectual property. Michael has a strong interest in the development of emerging technologies and the data economy, and is an active thought leader having published widely on issues to do with data, privacy and AI.

**Andrew Gray** is a partner in our Employee Relations & Safety team specialising in all aspects of employment and safety law. Andrew has worked closely with a number of clients to help them adapt to the workforce challenges arising from increased automisation and the future of work. Andrew is recognised for his expertise in handling sensitive high profile executive employment issues and is the "go-to" lawyer for many clients looking to implement senior executive change without legal or reputational risk.



**Kirsten Bowe** is a partner in the Mergers & Acquisitions team specialising in technology, intellectual property, data protection, new technologies and general commercial arrangements. She has extensive experience across a range of industries including telecommunications, infrastructure, government, health, energy and financial services. Kirsten has particular experience in large strategic sourcing and complex technology arrangements including outsourcing arrangements, complex technology development and implementation projects, agile projects and a range of cloud and managed services. Kirsten also has broad experience advising clients on data, privacy and cybersecurity issues in business operations (including the security of critical instruction legislation), in exploring new opportunities and in supporting M&A transactions. She also has a keen interest in new technologies including autonomous vehicles, drones, AI and machine learning.

**Peter Yeldham** is a partner in the Dispute Resolution team with a particular focus on insurance advice and claims. Peter has broad experience in financial lines and liability claims and policies (including cyber). In addition to his advocacy practice (that is, representing parties in respect of contested claims), Peter advises in relation to policy response, notification, claims management and policy wording in relation to professional indemnity insurance, directors & officers insurance, cyber insurance, public liability, and Industrial Special Risks policies. He is recognised by clients for his disciplined approach to meeting client commercial objectives, digestible advices and delivering value with his exceptional project management skills.

**Emma Newnham** is a senior associate in the Mergers & Acquisitions team. Emma specialises in both corporate governance and M&A work. She assists with annual reporting, AGM preparation and general head office advisory work and has experience in corporate restructures, capital raisings and company acquisitions. She works for clients across a range of industries and who are at different stages of their corporate journey.

**Rebecca Slater** specialises in intellectual property and technology law, regularly advising clients on intellectual property protection and licensing, data protection and general commercial arrangements. Rebecca has acted for clients across a range of industries, including technology, education, entertainment, energy and infrastructure, hospitality, and retail and banking. She also lectures at The University of Queensland on intellectual property, technology and privacy related matters. Rebecca has an LLM from Harvard Law School and is a trained mediator and facilitator.

**Cal Samson** is a solicitor in the Tech / IP team. Cal regularly advises on privacy and technology matters, including on privacy, data, surveillance and online content laws at the state and federal levels. Cal also provides advice on IP and IT contracting, and data and technology issues in M&A transactions, bribery and corruption, and modern slavery risks.

# Contents

Issue 3

# From the Editor


**Connect with KWM**
**www.kwm.com**
**Facebook** King & Wood Mallesons
**Twitter** @kwmlaw
**WeChat** @kwmlaw
**LinkedIn** King & Wood Mallesons

**Connect with KWM**
**Mark Beaufoy**
Partner, Melbourne
**T** +61 3 9643 4111
**M** +61 409 797 364
mark.beaufoy@au.kwm.com


## Climate and Cyber – Risks to real and virtual worlds dominate

**How are respondents to KWM's Directions survey thinking about the business environment?**

**63.6%**

**Cyber risk** is now clearly the No. 1 **"top of mind"** issue for directors and senior business leaders.

**51.4%**

Over half think it is very important that the Federal Government implement a **national emissions reduction policy,** including transitional targets for reaching net zero emissions by 2050.

# Foreword | The Climate conversation

**Hello and welcome to the third edition of NEXT**

A young publication, it has already witnessed the very change it was launched to prepare businesses for.

We've recently seen, through the release of the Sixth Assessment Report of the Intergovernmental Panel on Climate Change, an unequivocal assessment that humans have warmed the atmosphere, ocean and land.

At the same time, we have seen enormous change over the past 18 months in business' engagement on this topic and, particularly in an Australian context, businesses stepping in to make commitments to net zero in the absence of federal government action. Companies have been spurned to take action by their shareholders, their staff and their customers. Also more recently, the courts are playing a role.

Well over a decade ago, I worked on the first wind farm to be built on the Cape Verde archipelago. The project ended this small West African country's dependence on fossil fuel imports and produced immediate tangible environmental and economic improvements for this developing island nation. I became hooked on the positive impact that renewable energy and infrastructure projects can have on people's lives.

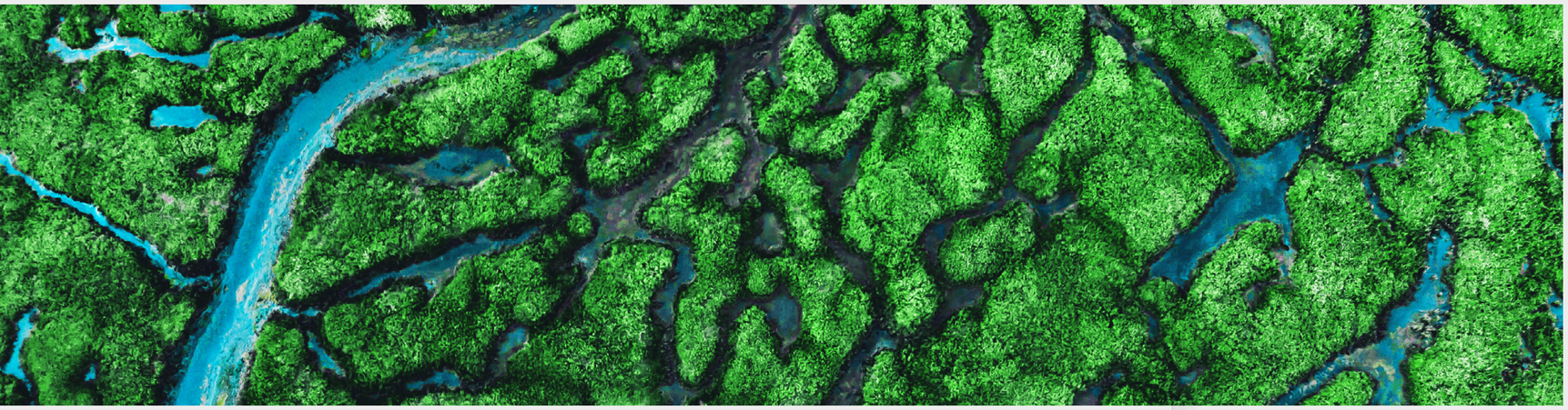
Of course, that project wasn't without challenges, but the rewards were worth the effort. Getting to net zero will be hard, but the rewards are great and the consequence of inaction significant.

It is challenging for companies as they navigate the increasing pressure to make ambitious net zero commitments against the risk of claims of greenwashing and ultimately litigation for setting targets that cannot currently be met or for which there is not currently a clear path.

The path to net zero will require creative ideas, technological innovation and a willingness from everyone to change old habits. It will also create amazing opportunities as people adapt and we transition to a low carbon future.

**Claire Rogers,**

Partner, Head of Climate, KWM



# Introduction

Hello and welcome,

I am delighted to introduce our third edition, full of thinking that expands NEXT's horizons.

The focus for this publication is providing our readers a bigger picture. We want to help businesses see what is next - appreciating the whole landscape to best enable successfully navigating it.

In this edition, our readers will gain a deeper perspective on emerging digitisation considerations around privacy, and cyber risk and its litigation potential. We look at the climate challenge from both business and political perspectives and take a different approach to exploring the communication challenge for any business facing a crisis. It is an exciting mix:

- **Kirsten Bowe** and **Rebecca Slater** look abroad to analyse the prospect that cyber incidents become cyber class actions. **Peter Yeldham** examines the insurability of those risks for organisations weighing them up.
- Continuing the digital theme, **Michael Swinson** and **Cal Samson** explains the implications for digital businesses (and consumers) from the Australian Information Commissioner's landmark privacy decision against ride-hailing and delivery provider Uber – a decision that provides insight into an interesting question on what it means to achieve global scale in a time of increasing data sensitivity.
- Looking up from the screen **Meredith Paynter** and **Emma Newnham** provide a deeper understanding of how Australia's biggest companies are facing the climate challenge, and how this is (literally!) redefining the notion of corporate social responsibility. Our research and explanation of the ASX50's approach to **ESG** (Environmental, Social and Governance) risks is a ready reckoner on the architecture and program building underway to address the climate imperative, which my colleague Claire Rogers has laid out in her foreword opposite.
- **Mark Beaufoy** explains the concept of the 'Green New Deal' and how climate and sustainability are already influencing the direction of economic recovery from COVID-19's ravages.
- Finally, **Andrew Gray** welcomes crisis communications expert **Gabriel McDowell** for a fascinating conversation on communicating in a crisis – the hypothetical scenario is both frightening and strikingly real. You can listen to this via podcast too.

Look out for more on technology and our future in forthcoming editions – we'll have deeper dives into the (legal and ethical questions for) emerging technologies like AI, and understand key elements of a low carbon future, like green financing.

I hope you enjoy this edition,

**Renae Lattey**


**Spotlight** Key takeaways from our climate change risk disclosures and governance analysis of the ASX50 in 2020. >>

# Spotlight

## Key takeaways from our climate change risk disclosures and governance analysis of the ASX50 in 2020

Meredith Paynter / Emma Newnham

### Overview

> While many things have slowed down due to the pandemic, the focus on climate change and climate change risk disclosures and governance has definitely heated up.

Our analysis of climate change risk disclosures and governance of the ASX50 in 2020 shows that ASX50 companies have generally been responding, and have set a new base line for climate change disclosures. Reporting against the recommendations of the Task Force on Climate-related Financial Disclosures (TCFD) is now the market standard among this group, with the Global Reporting Initiative (GRI) Standards and CDP (formerly the Carbon Disclosure Project) not far behind. Across their annual reports and dedicated climate change and sustainability/ESG reports, many companies are providing significant detail on the climate change risks and opportunities they face, including using scenario analysis to assess the potential implications of those risks.

Most ASX50 companies have set measurable targets and commitments, and most disclose how they are tracking against those targets and commitments.

Climate change governance has received significant attention, with most ASX50 companies having taken steps to embed climate change in their governance frameworks. Some of these companies have also introduced performance targets for executive remuneration tied to climate change metrics, reviewed industry association memberships for alignment on climate change policies, and obtained assurance from assurance practitioners on their climate change data.

There was, and will continue to be, investor and activist pressure to do more. 2020 saw a spate of shareholder requisitioned resolutions on climate change, and 2021 is shaping up to be even more heated.

This increasing focus is consistent with our Directions 2021 survey results, which focused on policy priorities for prosperity and growth, and demonstrated that respondents were comparatively more focused on ESG issues, including climate risks, compared to our survey results from prior years.

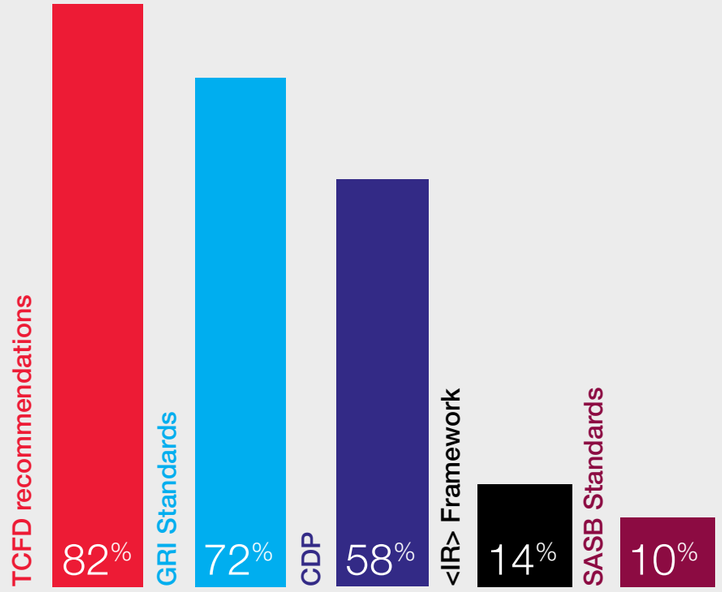
We also asked survey respondents to rate (on a scale of 1 – 10) the importance to business of the Federal Government implementing a policy (which includes transitional targets) to reach net zero emissions by 2050, and over 60% rated the importance of the issue at 7 or higher. As highlighted in Directions 2021, this indicates that there is strong support in the corporate sector for a nationwide commitment to carbon reduction commitments, consistent with actions being taken by many Australian corporates to achieve levels of carbon neutrality at either an organisational or product level. We also predicted that there would be more scrutiny of carbon neutrality claims as their importance increases and they become a business differentiator.

Our key observations from our analysis of climate change risk disclosures and governance of the ASX50 in 2020 are set out in this article.

We've also included some commentary on developments so far in 2021, as well as some predictions for what may lie ahead.

More detail of our analysis of climate change risk disclosures and governance of the ASX50 in 2020 is set out in our full report.

More detail regarding our Directions 2021 survey results is set out in Directions 2021 – Your Reform Agenda.




### Widespread voluntary reporting against global frameworks

The majority of the ASX50 companies (82%) reported against the TCFD recommendations in 2020, with a further 4% considering reporting against the TCFD recommendations in future.

The majority also reported in accordance with one or more other voluntary frameworks or standards including the GRI Standards, the CDP, the <IR> Framework of the International Integrated Reporting Council (IIRC) and the Sustainability Accounting Standards Board (SASB) standards.

From the second half of 2020 there has been significant movement towards a single global standard for climate change reporting. The International Financial Reporting Standards (IFRS) Foundation is trying to establish an international sustainability reporting standards board. That board would initially focus on climate-related reporting and build on the work of the TCFD, as well as considering a prototype climate-related financial disclosure standard proposed by a collaboration of five global framework- and standard-setters (including the GRI, CDP, IIRC and SASB).

### Most include disclosures on climate change risks in their operating and financial review (OFR), but disclosures vary significantly

While the majority of ASX50 companies (82%) are disclosing climate change risk in their OFR in their annual report, the extent of this disclosure varies significantly. We may start to see some more consistency going forward as companies refine their disclosures, including to address the results of ASIC's surveillance, APRA's vulnerability assessments and other initiatives.

### Majority are undertaking scenario analysis

The majority of ASX50 companies (74%) used scenario analysis to assess the potential implications of climate change risks. A variety of different scenarios were used, and there are differences of opinion as to which are the most appropriate. Some companies faced questions, including at their 2020 AGMs, on their choice and disclosure of scenarios.

## Growing number of targets and commitments

64% of ASX50 companies had made public measurable commitments in relation to climate change in 2020. Those that had made measurable commitments and targets generally included some disclosure on how they are tracking against their commitments and targets.

Already in 2021 we're seeing these numbers increase, with Coles Group committing to deliver net zero emissions by 2050 and Santos introducing new emissions reduction targets just prior to its AGM in April.

While these percentages may seem impressive, a number of these sorts of targets and commitments have been criticised in the media and other forums, including in shareholder statements accompanying requisitioned resolutions. The criticism largely focuses on whether the targets and commitments are scientifically backed to achieve the aims of the Paris Agreement. Few ASX50 companies (only 4) had their targets validated by the 'Science Based Targets' initiative in 2020. There are also differences in terminology (for example, net zero emissions v carbon neutrality) which are not necessarily well understood.

## Oversight of climate change risk is reflected in governance frameworks

The benchmark that directors will be held to in relation to climate change risk is rising. Australian regulators have publicly stated they are monitoring climate change disclosure and recent climate change related litigation has sought to test the boundaries of liability and change corporate and institutional behaviour in relation to climate risk. Recently published legal opinions also highlight the risks in relation to climate change and disclosure for directors, including remarks by The Hon Kenneth Hayne AC QC to the Centre for Policy Development's Business Roundtable on Climate and Sustainability and a series of opinions by barristers Noel Hutley SC and Sebastian Hartford Davis.

Most ASX50 companies have reflected oversight of climate change risk in their governance frameworks. Some examples include expressly referencing responsibility for climate change risk in the board charter, involving board risk and audit committees in considering and monitoring climate-related matters, establishing climate change working groups and steering committees and creating executive roles focused on climate change or sustainability matters.

## Companies linking executive remuneration to climate change

Shareholder requisitioned resolutions have called for links between executive remuneration and climate change targets for years. Some companies have taken steps to accommodate this. In 2020, 30% of ASX50 companies linked some elements of executive remuneration to climate change measures, with a further 10% linked to sustainability measures.

As with all things remuneration, you can't please everyone. Some proxy advisers objected to such measures on the basis that achieving climate change targets should be part of an executive's "day job" and shouldn't warrant a bonus. It may well be that some shareholders have expressed similar views privately.

The majority of the companies that link executive remuneration to climate change are in the materials, energy, real estate and financials GICS industry sectors. This was consistent with a number of other data points in our analysis, which tended to be skewed towards these sectors. These sectors are significantly represented in the ASX50.

## Industry associations coming under pressure to align on climate change

Likewise shareholder requisitioned resolutions at AGMs have been calling for several years for companies to review and report on industry associations' alignment on climate change issues.

In 2020, 40% of ASX50 companies disclosed their approach to industry associations in relation to climate change.

2020 also saw BHP and Origin Energy suspend their membership of the Queensland Resources Council over the Council's "vote Greens last" campaign.





## Assurance on climate change disclosures being obtained

52% of ASX50 companies obtained assurance on their climate change disclosures in 2020, such as scope 1 and 2 emissions data. In each case this assurance was provided by one of the big 4 accounting firms.

## Higher levels of support for climate change resolutions

Activists continued to make full use of their ability to requisition climate change resolutions at AGMs in 2020. These continued to take the form of a proposed amendment to a company's constitution followed by an advisory resolution contingent on the constitutional amendment being carried.

In 2020, 9 companies received requisitions for climate change resolutions and put them to the AGM. No climate change resolutions were carried in 2020. The average support vote for constitutional amendments among this cohort was just under 8%. But the level of shareholder support for the contingent climate change resolution was much higher – at just over 32%. In particular, the highest shareholder vote in favour of a climate change resolution was just over 50% – if formally put to the meeting, that resolution may well have passed.

The vote on these climate change resolutions sends an important signal to boards that climate change issues are important to shareholders. It may be partly in response to that sentiment that several boards in 2021 have begun to support climate change resolutions. We're seeing this in two ways. First, through boards adopting the "Say on Climate" initiative, and agreeing to give shareholders a vote on their climate change reports at their 2022 AGM. Following the announcement of this, the relevant requisitioned resolution is typically withdrawn. And secondly, through board support for climate change resolutions that will be put to shareholder vote at the 2021 AGM.

## Our dataset

In reviewing our data for 2020 we looked at annual reports, climate change reports and sustainability/ESG reports released in 2020 and other readily accessible publicly available information for companies that were in the S&P/ASX50 as at 5 February 2021.

More detail on our dataset is set out in our report.

## Authors

**Meredith Paynter**
**Partner**
**Mergers & Acquisitions**

**Emma Newnham**
**Senior Associate**
**Mergers & Acquisitions**

# Green New Deals

What does a **sustainable recovery** look like?

Aligning economic recovery from the COVID-19 pandemic with sustainability goals has been a focus in recent ‘Green New Deals’ developed in Europe and the US.

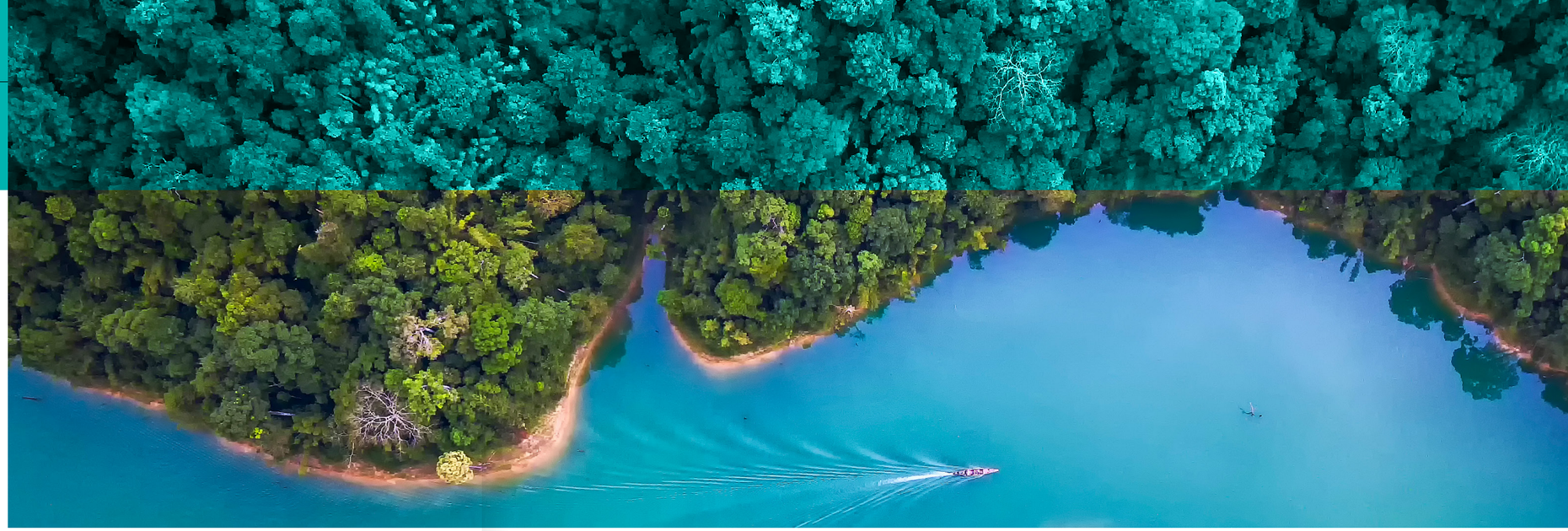
In this article we ask what role Green New Deals will play in a sustainable recovery from the COVID-19 pandemic globally, and assess whether they’ll influence the direction of change in Australia and Southeast Asia.

OPERATIONS

Author

**Mark Beaufoy**
**Partner**
**Environment, Planning & Native Title**

# Green New Deals



As the COVID-19 virus continues to evolve and extreme weather events increase in frequency, national governments face combined economic and environmental challenges. There is immediate pressure to prioritise economic recovery from the pandemic's ongoing impacts. The latest IPCC report underscores the urgent and ongoing requirement to improve responsiveness and resilience to climate-related natural disasters. Recognising the obvious limitations of mitigation measures to respond to such disasters and there is also increasing pressure to define a clear path for achieving the commitments of the United Nations Framework Convention on Climate Change (UNFCCC) Paris Agreement (Paris Agreement). Specifically, "holding the increase in the global average temperature to well below 2°C above pre-industrial levels and to pursue efforts to limit the temperature increase to 1.5°C above pre-industrial levels".

Having committed to meeting the Paris Agreement commitments and setting of 2050 climate targets, governments face budget constraints, questions around political will and the necessity of political compromise, and competing policy priorities. This is particularly so following the pandemic. But the pandemic, continuing climate-related disasters, the United States' direction under President Joe Biden is seeing these previously competing priorities of economic recovery, sustainability and climate resilience converge into an expectation for a 'sustainable recovery'.

The European and US New Green Deals and variants of this in our region provide a ready framework, with the focus on promotion of climate resilient infrastructure, low emission technologies and leveraging public and private finance to invest in clean energy and infrastructure. These central tenets of those compacts are also critical (if less quoted) elements of the Paris Agreement: "increasing the ability to adapt to the adverse impacts of climate change and foster climate resilience and low greenhouse gas emissions development, in a manner that does not threaten food production… and making finance flows consistent with a pathway towards low greenhouse gas emissions and climate-resilient development".

## The Theory

The concept of a 'green new deal' articulated by economic theorist Jeremy Rifkin was based on the emergence of the concept and plans in Europe and then the Green New Deal resolution introduced into the US House of Representatives in February 2019. According to Rifkin, it involves a comprehensive range of measures and initiatives to speed the transition of the economy and society to a low-carbon, sustainable and resilient future and address climate change. These include: a range of reforms to taxes and subsidies; tax credits and incentives for investment in renewables and low carbon technologies; enhancing electricity network connections; incentivising uptake of electric vehicles and installation of charging stations; green infrastructure and green buildings; sustainable agriculture; upgrading resilience of existing infrastructure to severe weather events; improving climate change-related disaster preparedness; leveraging investment and lending for the new green deal economy; education, training and research and development focused on the new green deal economy; and development of standards, codes and regulations which support this transition.

The key components emerging in many of the green new deal-like plans in the US, Europe, Japan and South Korea are carbon emission reduction commitments (net zero by 2050); fast-tracking of infrastructure, particularly low emissions technology (in energy projects, waste and resource recovery and smart cities); leveraging public and private money for low emission technology projects; and supporting transition to a green economy. This is consistent with recent strategies adopted by Southeast Asian countries at their November 2020 meeting (outlined below) and in many of the Australian policy responses and budgetary commitments (however limited) to economic recovery from the pandemic.

## Europe

The components of the EU Green New Deal agreed to by the European Commission includes three concrete actions: a Just Transition Mechanism to leverage public and private money, including via the European Investment Bank, to help those that are most affected by the move towards the green economy; delivery of a Sustainable Europe Investment Plan – mobilising €1 trillion of investment for environmentally responsible projects; and a proposed European Climate Law to make the net zero by 2050 commitment legally binding.

At the heart of this proposed law is a recently-revealed plan for carbon border pricing, which would tax goods imported into the EU based on the emissions created during production, unless already taxed in the country of origin.

## The United States

During the United States (US) election campaign, Joe Biden proposed policies similar to the EU Green Deal. As President, Biden has introduced a US$2 trillion clean energy and infrastructure plan. This includes the US electricity sector being entirely renewables-generated, and carbon pricing and border adjustment mechanisms. President Biden has re-joined the Paris Agreement and has set a national goal of net-zero emissions by 2050.

President Biden's push to transform the US economy over the next ten years is supported by a US$1.7 trillion budget. Within the targets, he seeks to achieve a "carbon pollution-free" energy sector by 2030. In April 2021, Biden further announced fossil fuel subsidies will be replaced by clean energy incentives. There are also discussions currently that the US will no longer financially support oil and gas projects abroad and imports will be subject to a CO2 border adjustment.

## China

Set in the context of China's goal to become a global superpower by 2050, China's 14th five-year plan sets two compulsory targets - a decrease of 18% for CO2 intensity and 13.5% reduction of CO2 energy intensity from 2021 to 2025. The plan also refers to China's long-term emission goals and the plan introduced, but did not set, a CO2 cap. Xi Jinping also announced China's new ambition to enhance its nationally determined contribution for 2030 under the Paris Agreement and to reach carbon neutrality by 2060.

The plan also seeks to increase the share of renewable energy consumption to 20% of the energy market by 2025. China's growth and energy consumption leaves open the possibility for it being the biggest market for renewable energy, however, it also continues to be the largest consumer of coal.

China continues to operate 3000 coal mines which combined is more than the US, the EU, Japan, Russia and India, and has more than 2000 under construction. In addition, there is discussion that Chinese emissions have not peaked as their economy is still growing and their growth is not disconnected to carbon emissions. Therefore, China's ability to achieve carbon neutrality by 2060 may be ambitious, but demonstrates ambitious climate action and a target that China is committed to achieving.

## Elsewhere in Asia

Japan and South Korea have both endorsed the net zero by 2050 target. Recent infrastructure investment in Southeast Asia potentially puts the region on the cusp of a Green New Deal. In a Disruptive Asia article 'A Green Recovery can make Southeast Asia an Economic Powerhouse', Megan Argyriou documents the leading position of China, Japan and South Korea in the development of low-carbon technologies and the growing opportunity in countries in the region including Vietnam, Indonesia and the Philippines.

KEEP READING >>

# Green New Deals

The 37th Association of Southeast Asian Nations (ASEAN) Summit held in November 2020 adopted an ASEAN Comprehensive Recovery Framework and Implementation Plan (Framework). It includes five key strategies: (1) enhancing health systems; (2) strengthening human security; (3) maximising the potential of intra-ASEAN market and broader economic integration; (4) accelerating inclusive digital transformation; and (5) advancing towards a more sustainable and resilient future.

The Framework states: "This Broad Strategy emphasizes that a return to 'business as usual' is no longer an option for ASEAN in the postpandemic world, and this paradigm shift will require ASEAN governments, businesses, and civil society to work collectively to enable systemic change needed by the region for a sustainable and resilient future."

As part of the European Green Deal, the EU committed to developing stronger 'green deal diplomacy', focussed on convincing and supporting others to promote sustainable development. On 1 December 2020, the European Union and ASEAN upgraded their relations to a 'strategic partnership'. The areas of cooperation of the strategic partnership include climate change and biodiversity, clean energy transition, smart cities, healthy oceans and environmental protection.

## Australia

The language of the green new deal has not as yet resonated in Australia, but there is growing recognition of the importance of sustainability and ESG (Environment, Social & Governance) objectives for businesses and the communities they serve. The Australian Climate Change Authority has released publications which focus on the role of low-emission energy in economic recovery from the pandemic, for example, 'Economic recovery, resilience and prosperity after the coronavirus' released in July 2020.

However, in comparison to the US and European Green Deal movements, Australia's development of climate policies to reduce greenhouse gases is poor. The Australian Government has not yet formally adopted a net zero by 2050 target, however all Australian States and Territories have committed to net zero emissions by 2050.

To meet Australia's obligations under the Paris Agreement, Australia would need to reduce emissions by a minimum of 26% by 2030. The Government's messaging has been to say it is focussed on 'technology not targets' – seeking to prioritise the means for achieving emissions reduction, ahead of setting objectives.

In the 2021-2022 Australian Federal Budget, the government will invest $1.2 billion to establish Australia at the forefront of low emission technology innovation and commercialism. This includes being able to fund the development of carbon capture technologies, supporting large industrial facilities to reduce energy consumption, support clean technology innovation and reduce costs and streamline the reporting requirements covered by the National Greenhouse and Energy Reporting Scheme.[1]

While Australia lags behind other developed nations in developing climate policies and mechanisms to harness them, Australia's relative strength is its abundance of favourable renewable energy sources. These include hydropower, ocean renewable energy, wind energy, geothermal energy, solar and bioenergy. Investment in renewable energy has increased over recent years due to government policy incentives, elevated electricity prices and declining costs in renewable generation technology. The largest renewable energy is hydro with increasing use of wind farms.

## Conclusion

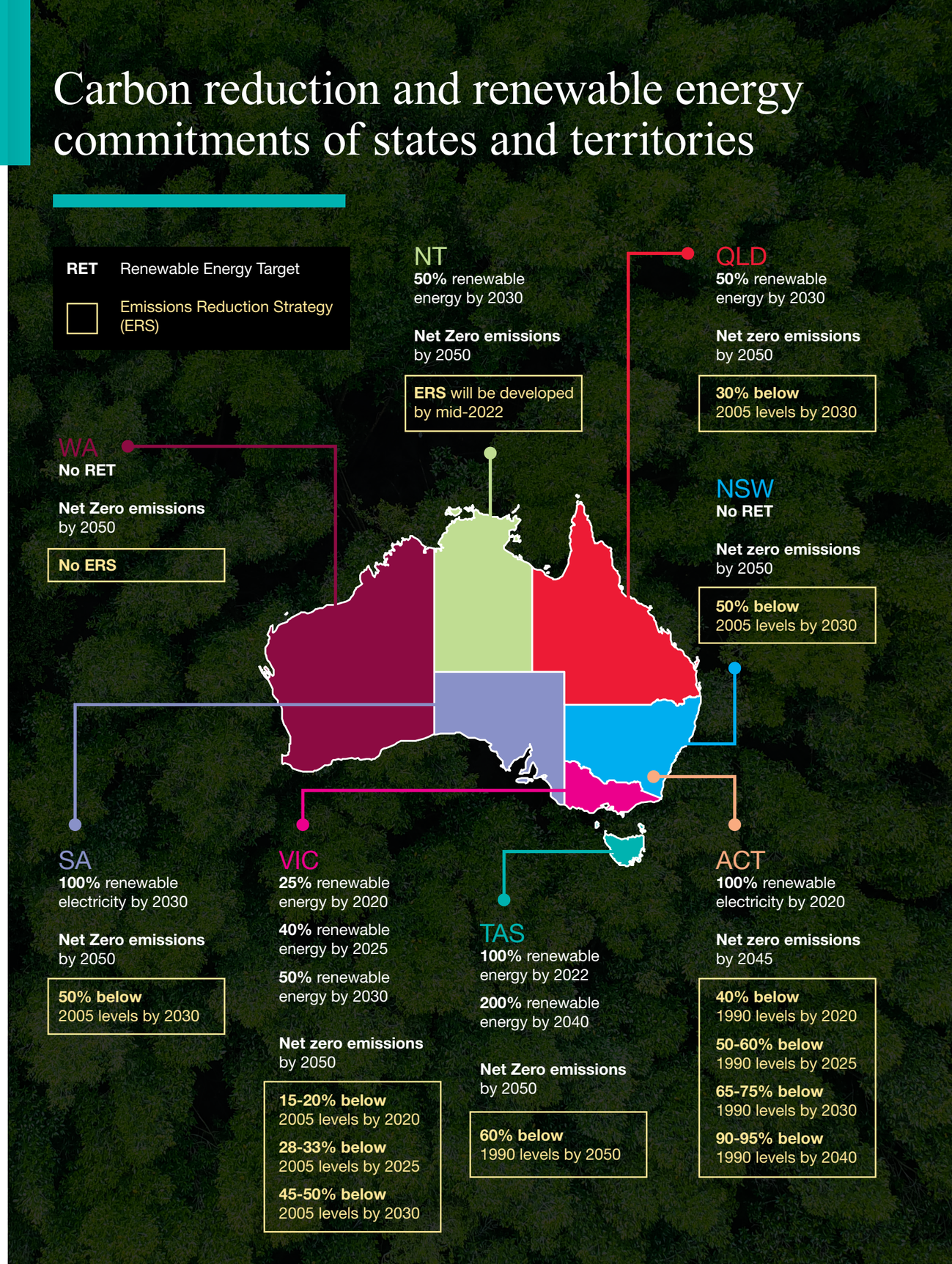
Climate mitigation and adaptation will be enormously expensive in the short-term, requiring trillions of dollars of investment in low-carbon and climate-resilient infrastructure. Governments cannot fund this transition. To bridge this gap in financial resources, the Paris Agreement expressly calls for mobilising private sector financing to support the enormous investments in green technologies and infrastructure that will be necessary to realise these sustainable transition and carbon emissions goals. ESG screening of investments and shareholder activism, and more recently climate change litigation, is influencing investment decisions. Sustainable finance (green loans and sustainability linked loans), corporate renewable power purchase agreements, green bonds (and the growing market of green, blue, climate, biodiversity, sustainability and social bonds) are playing a significant role in leveraging private capital. Multilateral development banks (such as the World Bank and Asian Development Bank) and the Clean Energy Finance Corporation in Australia, in conjunction with institutional investors such as superfunds, are catalysing private investment in a sustainable recovery.

Whether we like the terminology or not, the green new deal is coming to Australia and the region. The pace at which this occurs is likely to increase, as the USA, China and Europe's carbon reduction strategies evolve and feed into negotiations on addressing climate change at the UNFCCC Conference of the Parties (COP26) in Glasgow, UK in November 2021. Australia and Southeast Asian countries are well placed to deliver on the 'sustainable and resilient future' strategy of the ASEAN Comprehensive Recovery Framework, leverage existing knowledge, technology and experience and cooperate to deliver a low carbon transition supporting economic recovery and future growth in the region.

1. See Federal Government Budget 2021-2022

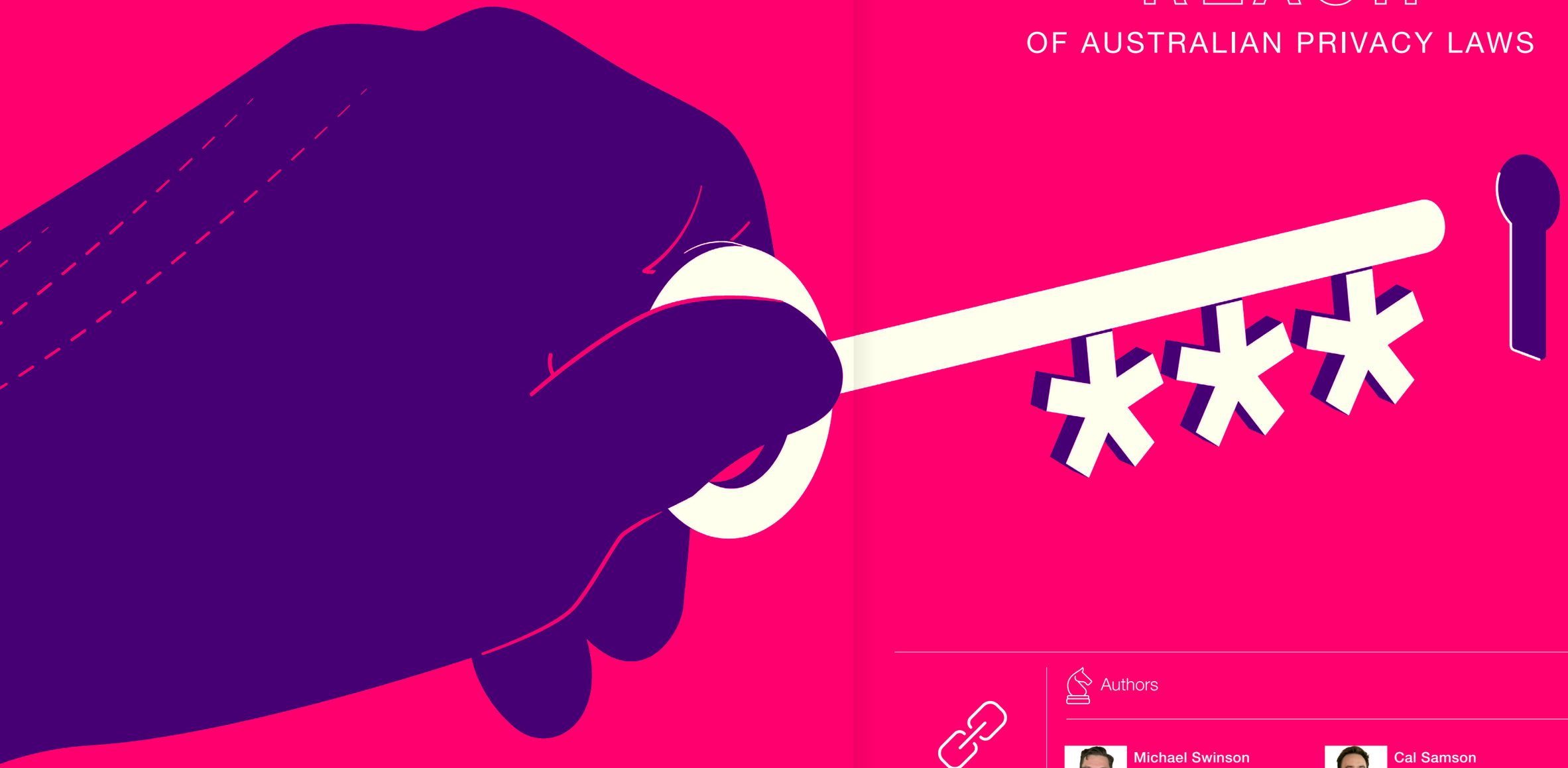


# Carbon reduction and renewable energy commitments of states and territories



# THE EXPANDING REACH

## OF AUSTRALIAN PRIVACY LAWS



RELATIONSHIPS

Authors


**Michael Swinson**
Partner
Tech and IP

**Cal Samson**
Solicitor
Tech and IP

**Dealing with an overlapping patchwork of disparate and sometimes contradictory privacy laws is a challenge for any multinational business. The challenge is even greater for online businesses that operate across multiple jurisdictions via a single platform (after all, the internet knows no jurisdictional boundaries). As torrents of information from around the world flow across digital platforms, it is increasingly difficult to keep track of what compliance requirements apply, particularly where domestic privacy laws have extra-territorial effect and domestic regulators claim jurisdiction over global operators.**

**A recent determination by the Australian Information Commissioner, after an extensive multi-year investigation, against Uber serves as a cautionary reminder to global corporations of the scope of their potential exposure to Australian privacy laws, even if they have limited or no physical presence here. These issues are likely to be tested again in the context of the Commissioner's ongoing civil penalty proceedings against Facebook in relation to the historical Cambridge Analytica incident (albeit that those proceedings are still at a relatively preliminary stage and are unlikely to be resolved for some time) and it is also possible that this area of law will be simplified as part of the Government's ongoing review of the Australian Privacy Act. However, for now, the Commissioner's analysis in the Uber determination serves as the clearest view of how the current laws will be applied in practice.**

## Background

In her determination, the Commissioner found that the US-based Uber Technologies, Inc. (**Uber**), and its Dutch-based subsidiary Uber B.V. (**UBV**), each failed to appropriately protect the personal data of Australian customers and drivers, which was accessed in a cyber-attack in October and November 2016 (**Uber Data Breach**).

Specifically, the Commissioner found that each company:

a. had an 'Australian link' and therefore was within the jurisdiction of the Privacy Act; and

b. breached the Privacy Act as each failed to comply with their obligations under APPs 1.2 (in relation to practices and procedures), and 11.1 and 11.2 (in relation to security).

## Extra-territorial application of the Privacy Act

Uber and UBV are respectively incorporated in the US and the Netherlands. Accordingly, the first substantive issue for the Commissioner was whether each company had an 'Australian link' such that they would be bound by the Privacy Act in relation to activities carried on outside Australia under the relevant jurisdictional 'hook' in section 5B of the Privacy Act.

In that respect, the Commissioner was required to be satisfied that, at the time of the Uber Data Breach, both UBV and Uber each: (a) carried on business in Australia; and (b) collected or held the relevant personal information in question in Australia.

In respect of UBV, the Commissioner had no difficulty establishing, and it was not in dispute, that UBV carried on business in Australia and collected personal information from Australian users. At the time of the Uber Data Breach, UBV was, for regions outside of the US, both the data controller for and licensor of the Uber app, and entered into direct contractual arrangements with both Australian riders and drivers. The Commissioner held that, despite being incorporated in the Netherlands and having no physical presence in Australia, UBV clearly had an 'Australian link'.

The equivalent analysis for Uber was less straight-forward, and Uber strongly disputed that it was subject to the jurisdiction of the Privacy Act. The Commissioner accepted that Uber did not have a physical presence in Australia, was headquartered in the US and did not have a direct contractual relationship with Australian riders or drivers at the time of the Uber Data Breach. Notwithstanding this, the Commissioner considered that Uber carried on business in Australia because it:

- installed and managed authentication, security and localisation cookies and similar technologies on Australian users' devices;
- rolled out new solutions (such as services, products, safety features, and troubleshooting) developed in the US on an international basis, including to Australia; and
- used centralised and global tools to enable UBV to carry out ad campaigns for Australian users.

The Commissioner relevantly held that it was not determinative that some or all of these acts may have been instituted or controlled remotely, or that they were done on behalf of UBV rather than on Uber's own behalf. Rather, touching upon requirements developed in previous case law on carrying on business in Australia, the Commissioner held that these activities demonstrated that Uber was engaging in activity in Australia, which was in the nature of a commercial enterprise, and which had a repetitive and permanent character.

The Commissioner also found that Uber collected personal information from Australian users in Australia. While UBV controlled the direct relationship with those users, in practice, data from those users was transferred straight to servers controlled and owned by Uber in the US. As such, the Commissioner was satisfied that Uber collected this information at the same time as it was collected by UBV – in other words, there was a simultaneous act of collection by the two entities. Combined with the Commissioner's conclusion that Uber was carrying on business in Australia, this meant that Uber had an 'Australian link' and was, therefore, bound to comply with the Australian Privacy Act in relation to its handling of information about Australian users.

## Breaches of the APPs

The Commissioner found that both Uber companies breached the Privacy Act for failure to comply with their obligations under the APPs. In particular, the Commissioner found that both companies interfered with the privacy of the affected Australian users by failing to take reasonable steps in the circumstances to:

- protect their personal information from unauthorised access, in breach of APP 11.1; and
- destroy or de-identify their personal information once it was no longer required, in breach of APP 11.2.

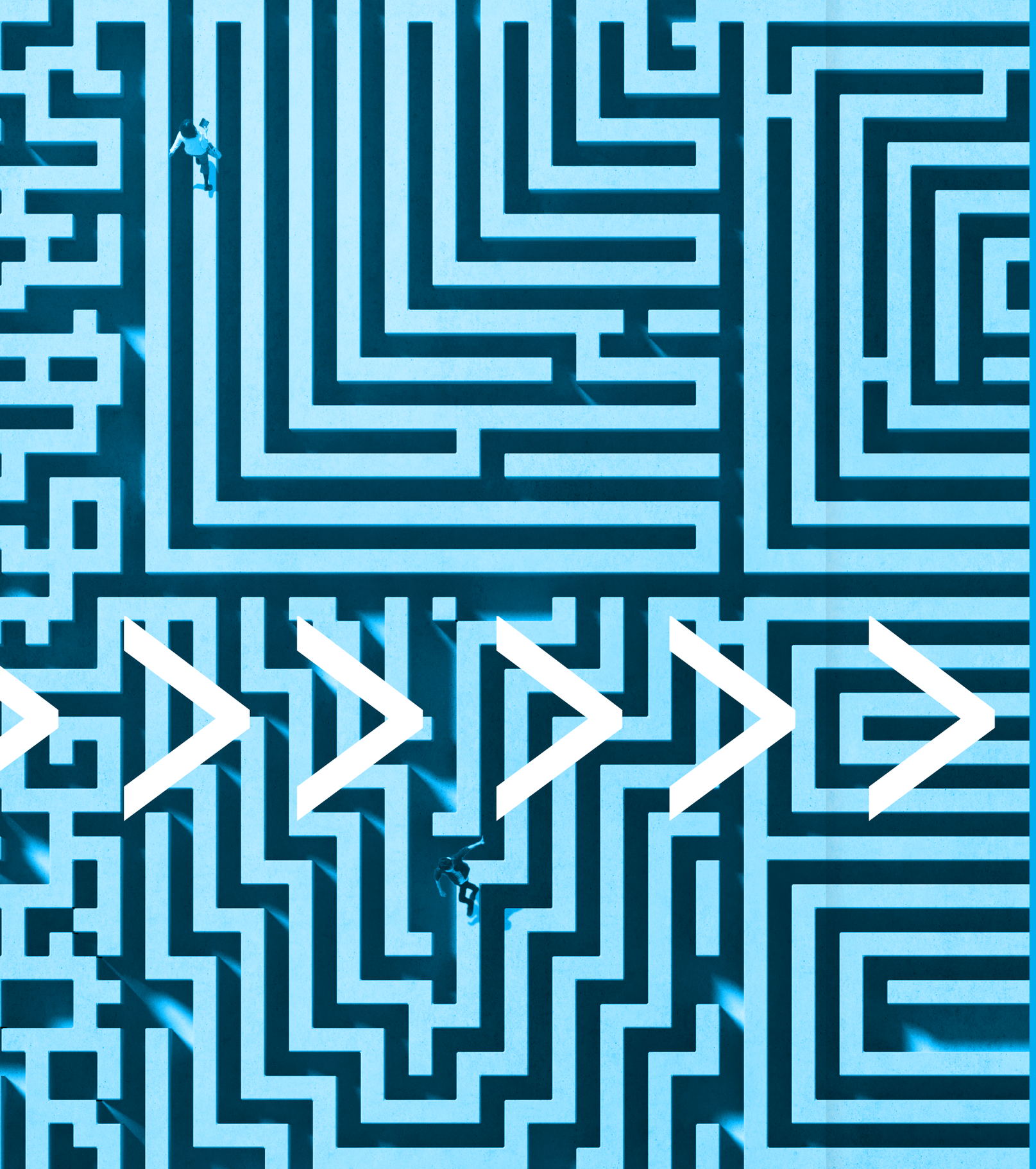
Further, the Commissioner held that both UBV and Uber failed to take reasonable steps in the circumstances to implement practices, procedures and systems relating to the Uber companies' functions and activities, to ensure compliance with the APPs, in breach of APP 1.2. From UBV's perspective, it was not sufficient to simply outsource these compliance obligations to Uber, with Uber being primarily responsible for the operation of the underlying technology platforms, given the substantial amount of information about Australian users at stake and foreseeable security risks. That is, some level of oversight by UBV was still required.

As a result, the Commissioner ordered the companies to prepare, implement and maintain a data retention and destruction policy, information security program, and incident response plan to ensure compliance with APPs 1.2, 11.1 and 11.2 respectively and to appoint an independent expert to review, report and provide recommendations on these policies and programs and their implementation, and submit the reports to the OAIC.

The Commissioner noted that while both UBV and Uber have already been subjected to regulatory action in other jurisdictions in relation to the Uber Data Breach, it was still appropriate and proportionate to take further action in Australia. In reaching this conclusion, the Commissioner indicated there was a public interest in making a declaration on these matters, noting that there were: "*complex issues that are specific to the Australian legislative context, including the application of the extraterritorial jurisdiction provisions in the Privacy Act to companies that outsource the handling of Australians' personal information to companies within their corporate group through 'data processing' agreements or similar arrangements*".

### Key Takeaways

- This determination serves as a significant statement by the Commissioner as to her view on the extraterritorial application of the Privacy Act. She has publicly stated that it *"makes my view of global corporations' responsibilities under Australian privacy law clear"*. As such, global businesses (parent companies and subsidiaries alike) with users in Australia should be on notice that they may be required to comply with Australian privacy laws.
- In the Commissioner's view it is clear that having no physical presence in Australia and no direct contractual relationship with Australians is no barrier to international entities from falling within the jurisdiction of the Privacy Act if they otherwise have sufficient connection with business activities that take place here. Uber has indicated that it will not appeal the Commissioner's determination, so it remains to be seen whether the courts will agree with the Commissioner's views.
- An entity cannot outsource compliance obligations under the Privacy Act simply by outsourcing relevant data processing activities to a related entity, or indeed to any other entity. The outsourcing entity will need to maintain an appropriate level of oversight and involvement to ensure that there is no privacy breach by the service provider for which the outsourcing entity may ultimately share some responsibility.
- Global businesses may still face regulatory action in Australia, even if they have been subject to similar actions in other jurisdictions.



CYBERSECURITY

# CLASS ACTIONS

GOVERNANCE

**In recent years we have seen a sharp increase in the prevalence and impact of cybersecurity incidents. In our recent Directions survey, managing IT and cyber risk was the leading issue of material concern for respondents. And if trends in the United States are any indication, there could be reason for concern. Trends in Australian fashion, music and film often mirror those of the United States. This can also be true of legal trends. Can Australia look to the US to predict what is coming in the cybersecurity (or data breach) class action space?**

>>


Authors

**Kirsten Bowe**
Partner
Corporate M&A

**Rebecca Slater**
Special Counsel
Corporate M&A

# A (SHORT) HISTORY LESSON

The tort of privacy was developed in the US in the late 1890s off the back of increasing circulation of newspapers and rapid technological advancements, including the handheld camera. The Kodak company introduced the first mass market camera in 1901, at a price point accessible to the general public. Journalists and ordinary people were able to photograph other people in public places for the first time.

Fast-forward to 2021 – and the Australian Attorney-General's Department is considering the introduction of a statutory tort of privacy as part of its review of the *Privacy Act 1988* (Cth). From the bench, Justice Keane has recently commented that it "would not be surprising" for the High Court to accept a common law tort of privacy along US lines.

The US also led on the tort of negligence, which was developed in the US in the 1920s. The tort of negligence found its way to Australian courts some 10 years later.

How about class actions? "Equity Rule 48" was passed in the US in 1833. This allowed for "representative litigation" to be carried out when a multitude of similar individual cases had been filed, in the interests of both justice and convenience. Unsurprisingly, this coincided with the Industrial Revolution. New manufacturing processes were advancing faster than workplace safety measures. This resulted in many workers suffering similar injuries. These workers were of limited means, and unable to sue individually. The 1950s were also a key period for class actions in the US. Civil rights and environmental activists used class actions to provide visibility to their causes. A key case during this period was *Brown v Board of Education of Topeka*, which held that segregated schools were unconstitutional.

The first class action regime was enacted in Australia in 1992, when Parliament amended the *Federal Court of Australia Act 1976* (Cth) to enable class actions to be run in Australia.

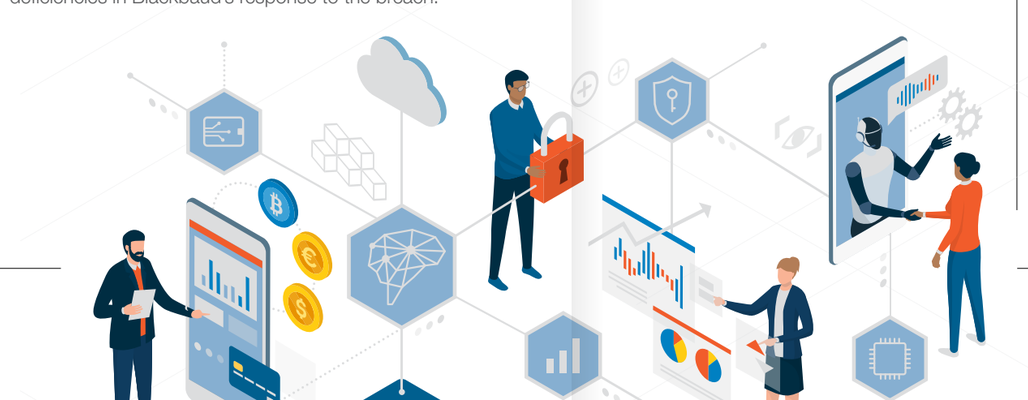
## CURRENT CYBERSECURITY LAWSUITS IN THE US

In the US, a lawsuit arising from a data breach may rely on a number of different causes of action. Where a service provider is involved (for example, a cloud provider that stores customer data for a hospital), the individual affected by the data breach may sue either or both the service provider and the data controller (in our example, the hospital).

*Allen v Blackbaud Inc.* is an example of a class action suit against an IT service provider. Blackbaud describes itself as "the world's leading cloud software company powering social good". It manages servers for not-for-profit organisations, educational institutions and organisations in the healthcare space. It was subject to a three-month ransomware attack which began in February 2020. (Ransomware is a form of malware that locks down a system of individual files until a ransom is paid. Often the attacker takes a copy of some or all of the files before locking them and threatens to publish or sell them on the dark web if the ransom is not paid.) The attack exposed the personal information of students, patients, donors, and other individuals – all of which were customers of Blackbaud's customers. Blackbaud paid the ransom, and was then sued. The class in the resulting class action suit is comprised of individuals whose data was accessed (and not Blackbaud's "direct" customers, such as universities). The suit identified the following deficiencies in Blackbaud's response to the breach:

- Blackbaud did not provide the affected individuals with timely notice of the breach. It notified users months later in July and August 2020.
- It failed to identify all of the information that had been accessed. Initially, Blackbaud had claimed that bank account information, social security numbers, usernames and passwords had not been compromised. This was corrected by Blackbaud in a Form 8-K filing in September 2020.
- Blackbaud had not properly monitored its IT systems, and this had delayed its awareness of the incident.

The affected "customers of customers" relied on the following causes of action: negligence, breach of privacy, breach of contract (both express and implied), and violations of relevant state data breach legislation. Damages were claimed for the costs of ongoing credit monitoring and potential future losses arising from identity theft.



A review of recent US cybersecurity lawsuits reveals the following trends:

- Class action suits are common where a data breach impacts multiple people or businesses.
- Many class action suits are being filed off the back of ransomware attacks.
- Where a service provider (for example, a cloud provider) is the cause of the breach, the limitation of liability provision in the relevant contract will be analysed. In many cases, the relevant provision will not have contemplated a cybersecurity incident. This has raised some interesting questions. For example, US courts have been asked to consider whether loss of data should be regarded as a loss of property.
- It can be difficult to identify the responsible entity (i.e. the entity that caused the harm) where a service provider has a complex corporate structure.
- It is difficult to know what harm may arise in the future due to a data breach today. In light of this, many claims are for potential future losses or to cover the costs of ongoing monitoring activities.
- However, plaintiffs bringing such claims may not have sufficient standing. US federal courts may not have jurisdiction to hear "speculative", "conjectural" or "hypothetical" claims. This means that, for example, the mere possibility that a plaintiff's credit may suffer if a hacker opts to sell or release this information to those able and willing to exploit it cannot impart the requisite standing.
- Most (but not all) class action settlements for cybersecurity breaches have a global cap on damages.
- There have been instances in the US where the cybersecurity expert engaged to identify and close out the vulnerability has been sued.
- Shareholders of US companies are suing directors for data breaches.
- Similar to the trend we are seeing in Australia, regulators are bringing lawsuits against large, often multinational, companies who have suffered a data breach.
- It is tricky, and consequently rare, to go after a hacker. They are difficult to locate, and even if they can be tracked down, jurisdictional issues are likely to arise.
- In many cases, it appears that the standard of care expected of both organisations and service providers is high.

# WHAT'S HAPPENING IN AUSTRALIA

Recent experience in Australian class actions suggests that regulatory action often leads to increased private litigation risk. In recent years, we have seen both the ACCC and the OAIC commence regulatory action against the likes of Facebook and Google. High-profile data breaches are also on the uptick, and data breaches overall were trending higher in 2020. Class actions generally are increasing in prevalence in Australia.

Australia's first privacy-related class action was brought by NSW Ambulance officers in November 2017. A contractor unlawfully accessed personal information of 130 officers and sold the information to personal injury law firms. The claimants alleged that NSW Ambulance was liable for breach of confidence, breach of contract, misleading or deceptive conduct and invasion of privacy. The NSW Supreme Court approved a $275,000 settlement in that case. This case did not involve a cybersecurity breach.

There has been an increase in the number of cybersecurity class actions being investigated by Australian law firms.

The same law firm that represented the ambulance officers is currently investigating a class action against Service NSW in relation to the theft of the personal information of 103,000 customers by hackers in a phishing attack on employee email accounts.

The causes of action available to US plaintiffs have been canvassed above. The legal bases for Australian cybersecurity class actions have not yet been considered by the Australian courts. There is currently no tort of privacy in Australia and no private right of action for a breach of the *Privacy Act 1988* (Cth). However, the High Court indicated in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* that it may be receptive to arguments that a common law right of privacy should be recognised in the future. In the event of a data breach, other causes of action available to an Australian claimant may include (depending on the circumstances of the breach): breach of contract, negligence, breach of confidence, and claims based on general statutory obligations (for example, misleading or deceptive conduct or breach of a company's continuous disclosure obligations).

The Australian Government's ongoing review of the *Privacy Act 1988* (Cth) has sought public consultation on the potential to introduce a direct right of action for individuals as well as a statutory tort of privacy. The Issues Paper published by the Attorney-General appears to lean towards the introduction of a direct right of action as the appropriate mechanism to deal with serious breaches of privacy. Such a mechanism would give standing to classes of individuals to bring an action against regulated entities for widespread or systematic cybersecurity incidents.

When cybersecurity class actions begin to be litigated in Australia, the courts will need to determine the standard of care (ie. what constitutes reasonably prudent cybersecurity practices). In 2021, security is not absolute, hacking attacks are increasingly in prevalence and sophistication, and industry standards are continually evolving. What reasonable steps should organisations (including service providers) be taking to prevent security breaches? If current US trends find their way to Australia, the standard of care will be high. Organisations and IT service providers will be expected to be informed and proactive in relation to managing cybersecurity risks. ■

# CYBER INSURANCE

## What do you need to know?

There are three broads lines of risk management for cyber incidents in Australia. The first is to educate and train staff. The second is to build, monitor, safeguard and regularly test IT infrastructure and applications. The third is to have cyber insurance. The first two can prevent loss, the last is only reactionary and can only be used to recover losses.

Cyber insurance is an important risk management tool in Australia. Cyber insurance can be purchased as a bespoke insurance product or packaged together with another insurance policy (such as professional indemnity insurance, or a policy providing for business interruption loss).

A cyber insurance policy will ordinarily provide insurance cover for **first party losses** (that is, the direct losses of the policy holder in responding to a cyber incident or attack). First party losses include the cost of repairing or remediating impacted IT systems; the fees for third-party forensic experts to identify and quantify the impact of a cyber incident; and, in some circumstances, the cost of extortion payments or ransoms. Policy holders and insurers may agree in advance which forensic experts or third-party advisors can be engaged in the event of a cyber incident.

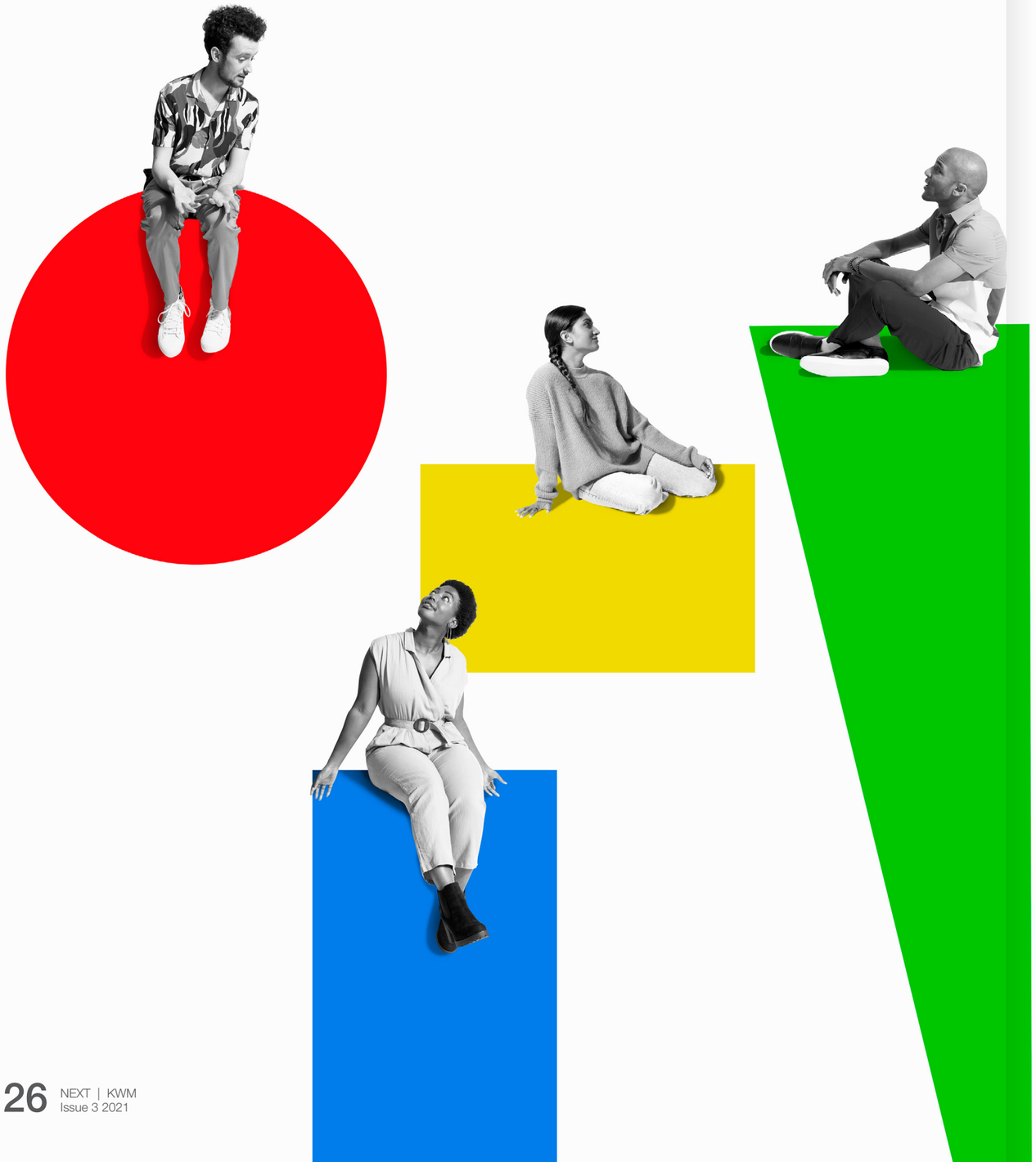
A cyber policy may also provide cover for **third party losses** (that is, indirect losses caused as a result of a cyber incident) including the cost of derivative litigation (which could be brought by the policy holder's customers for breach of contract in failing to protect personal information) or fines imposed by regulators for statutory breaches. As ever, the extent of insurance cover will depend on the policy wording, and policy limits.

If a cyber incident occurs, notification of the incident should be promptly made to insurers (some policies will require notification within a prescribed period), and we recommend regular engagement with cyber insurers as the cyber incident is investigated and contained.

**Peter Yeldham**
Partner
Dispute Resolution

# Communicating in a Crisis

## KWM & ResPublica



**Picture this…** your business has just suffered a major safety incident. Details are still emerging. Rumours are swirling, media are bombarding you with questions. Your reputation is on the line and to top it off, it's New Years Eve.

As a matter of fact, a client of KWM Partner **Andy Gray** faced this situation. Andy called in ResPublica PR's **Gabriel McDowell**. In this article, KWM Corporate Affairs Manager (and former journalist) **James Bennett** asks them both to navigate a hypothetical scenario, to explain a few of the key principles to communicating in a crisis.

>>

Authors


**Andrew Gray**
Partner
PE M&A

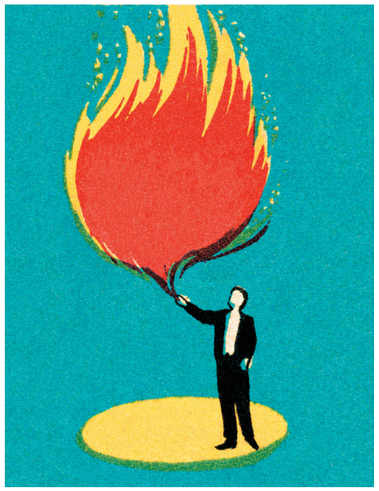
**James Bennett**
Corporate Affairs Manager
Communications

**Gabriel McDowell**
Executive Chairman
ResPublica

# Communicating in a Crisis

Below is an edited transcript of a podcast conversation between Andy, Gabriel and James, which you can access here.

**Andrew Gray** I'll explain why we've picked this hypothetical. It's a major workplace safety incident which is my area of practice but it also has a possible cybersecurity angle. And that's topical when you look at our recent Directions survey, which asks business leaders about the issues they face - they saw cyber risks, including those arising from rapid digitisation to be the number 1 concern by a significant distance. Previously it had sat behind brand and reputation, but it has really skyrocketed in this survey. And equally anyone who has some experience with a workplace fatality will be conscious of the impact that can have on the business and also the personal impact it can have on individual management teams and the first responders and their family members as well.



**James Bennett** Thanks Andy. Here we go:

**THE SCENARIO**

- A fire has broken out after an incident at the Benign Chemicals Co on the city's outskirts. Three employees have been killed.
- One is injured but escaped, and another is missing in the affected plant area.
- Firefighters are urging people in the suburb downwind to leave if they can out of concern that those with breathing difficulties may be affected.
- The police and WorkCover are already on the site investigating and are seeking to grill a distressed management team on what happened.
- The EPA has released a statement saying it has commenced an investigation as well. An opposition politician is tweeting erroneous claims that Benign failed a recent safety and cybersecurity audit. The union is protesting about an apparent decline in safety conditions.
- The plant's operator is coming to you, Andy and Gabriel, for advice.
- She confides that she and two senior managers had received a threatening email a week or so ago which claims to have compromised the plant's production control software.
- An external cybersecurity agency conducted a threat assessment and found no vulnerability and recommending no further action.

**AG** There is a lot in that, safety issues, some environmental issues, cyber issues. Gabriel, being a lawyer our natural instinct is to avoid risk by keeping our head down where-ever possible, but focussing on the legal risks in these situations can create some issues as well, what's your view from a PR perspective on the initial response?

**Gabriel McDowell** The first thing that I would say, we as communication professionals have to get the CEO focussed on what the key task is, and the key task is to assist the authorities in terms of minimising any harm to employees or people in terms of communicating early in the piece. You would be encouraging everybody to actually go to official channels for information. So you would be helping them do that job and demonstrate that you are focussing on the one priority, which is the safety and concern of your people, and make sure everybody is safe. That's our number one priority. You need to communicate that regularly and constantly and say that's where your focus is - to communicate that they are taking care of matters as they should be in the health and safety of the people number one, and that they're on top of the situation and done an investigation assisting authorities to get to the bottom of the real issue, which is that threat to community in terms of environmental disaster, potentially.

**JB** And there's a whole range of stakeholders involved?

**GM** There's a hierarchy. Those who are directly affected, which would be the employees in the community and the families of your employees. You're going to have to figure out how quickly you can communicate to them, and those other community stakeholders. You won't be able to do that with them all immediately, so using the media, electronic media particularly, and social media, in the early days is going to be pretty important.

## Three elements of response

**AG** I think there's three main elements - the legal response, the communications response and then there's employee wellbeing response as well. All of those issues need to be front of mind when you're dealing with an incident like this. Legal issues in some respects are secondary, but there are a number that we need to be thinking about when an incident like this occurs. Obviously, the immediate priority is making sure everyone is safe, making sure that regulators are provided the information they need and relevant notifications are made. One critical thing is that there's a single point of contact nominated from the company's perspective, to deal with either media representatives or regulatory representatives, whoever it might be. But Gabriel, although I'll be cautious about handing the information over to regulators, clearly that doesn't prevent your organisation from speaking publicly. What are the key principles the organisation should apply in its public stance?

## Communication principles

**GM** One of the key things in terms of the communication perspective, is to communicate that it is being treated with the seriousness that it deserves, so if there is a crisis or major issue, that demands the CEO or somebody very senior seen to be the front in facing this. The biggest mistake is under communicating in the early hours of a crisis. Even if you don't have all the facts. In this particular case we know some of the facts so you can share those. You know that phrase, nature abhors a vacuum? So does the media, there's a rumour mill and if you step away, somebody else will fill that gap and your chances of controlling the communication agenda will evaporate if you don't get on top of it early. Communicate regularly. Over communication is much better than under communication.

I haven't seen it arise for close on a decade now, but I used to get - not with KWM - a situation where a lawyer would say don't apologise. Well you do apologise. I don't think an apology is necessarily an admission of some sort of legal liability.

A lack of control over social media in the early days is something to watch particularly for B to B corporations who aren't really across social media as a communication tool. So having somebody that can quickly get to grasp with that space for you is, this is pretty important.

Impatience is an issue too. This scenario could go on for weeks and months as new information or investigations unwind. The worst case of impatience was the BP disaster in the Gulf Mexico where the CEO went sailing whilst the issue was still alive, and when asked by the media about this he said I want my life back. That just showed a lack of empathy for people whose lives and livelihoods had been destroyed.

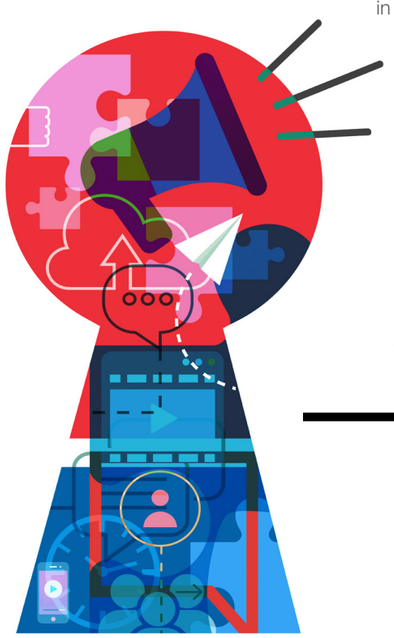
# Communicating in a Crisis

## Take it seriously

**JB** That's a really interesting point, it goes to the point that you make about the perceived seriousness - a CEO who is creating a perception that he's more concerned about his own work/life balance?

**GM** Yes early in that piece they suggested that the explosion may have been caused by a contractor for them, so again it looked like they were trying to dodge responsibility so those were two real no no's. In those situations I would say well ultimately we are responsible and ultimately at the moment my focus is on trying to help the authorities get to the bottom of this so it doesn't happen again, and that you know you can handle the fire again putting the liability on yourself but at the same time that suggests that you're somehow trying to dodge a responsibility.

**JB** Andy and Gabriel you're now about to join a call with the plant's General Manager. Her phone's obviously ringing off the hook and you can appreciate the level of stress knowing the people that have been directly affected. What do the key messages need to be?



## Key messages

**GM** It's really getting them to focus on the known facts as they impact the audience or the particular group of people that they're going to address and try as much as humanly possible to stick to that whilst you know demonstrating you're really concerned about what they're going through. That's the key to this, and not being afraid to say "well I don't know that that's true, that's speculation, you can appreciate I really need to deal with the facts as we know them right this minute".

**AG** Speculation is dangerous. I think that's the key message I provide in these sort of scenarios, don't speculate. Avoid the temptation to try and figure out the answer before you know it and communicate that, because there'll be a great amount of pressure being applied from a range of stakeholders and speculating and getting it wrong just comes back to cause problems in my experience. And then the other thing is to focus on employee wellbeing and your own wellbeing. People often forget about the general manager or the CEO whoever it is. I've seen that before - everyone else gets counselling except for the person at the top who is probably bearing the brunt of this incident in a whole different variety of ways so be mindful of that.

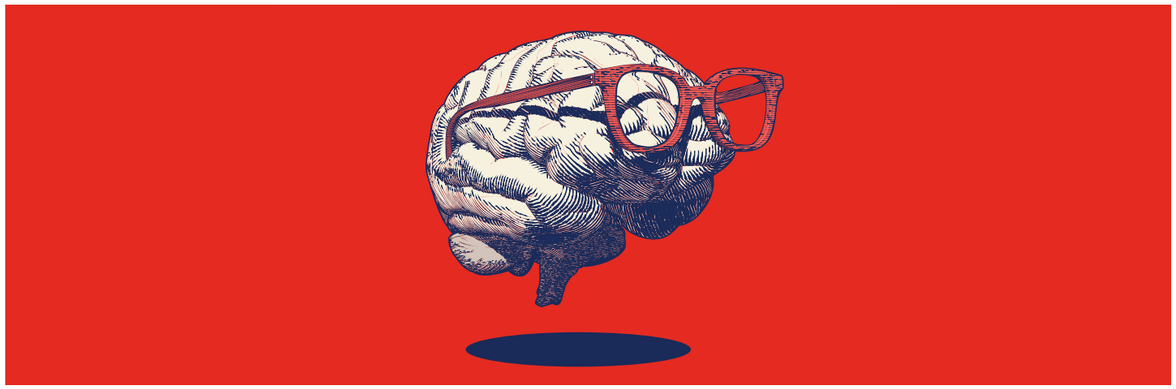
## Media management

**JB** Dealing with media. It is easy to think of media as a holistic entity, but individual journalists are each going to have their own needs - some might be working for just a written news service who'd be happy with a couple of comments, others might be saying, you know can we get your GM on the phone to talk about it. You've got a range of different interests within media. So how would you think about going to manage something like that Gabriel in a situation like this?

**GM** You want to figure out how you can knock off as much as you can in the shortest space of time as you can. Both for the media but also your spokesperson who in this case is your CEO – there is a range of other issues they must manage. Have a plan of action gives people what they need. Have somebody who's professional and understands those needs and can follow up with journalists and give supplementary information. They need to fill that 30 seconds of TV or that 3 minutes of TV. Reassure journalists they are going to get what they need from you, and they do not have to go and unnecessarily interview ten other people instead of one or two other people as to what their perspective is when they may or may not have a necessarily valid perspective. As I said, media abhors a vacuum.

**JB** From first-hand experience, instilling in a media pack the sense that an organisation is trying to be helpful and as upfront as it can be is really very impactful in the way that media respond in terms of whether they take explanations at face value or go searching for an alternative story which, as you say, leads into the risk of speculation.





**GM** Absolutely. It is building trust. You know, (assuring people) "he doesn't have all the answers, but he is being honest with us and he's facing up to us and he understands what we need". It is so, so important in those circumstances.

## Honesty

**AG** The client's relationship with their advisors needs to be honest and open as well. There is nothing worse than finding out a piece of information after it's brought to your attention by a regulator or after it's brought to your attention by a journalist and you are on the back foot. With individuals involved in the incident, you need to create an environment where they feel that they can be open and honest with their advisers about what's occurred. Because our role as an adviser is only ever going to be as good as the information we are given. If people feel it's a blame game or there is a lack of trust between the advisers and the management team, you will get a sub-optimal outcome and we have seen that in the past. I think that's an important thing to keep in mind as well.

## The next phase

**JB** Looking forward, there are going to be regulatory investigations that kick in. What additional considerations then apply, are there other advisor roles that are useful? Government relations, for example?

**GM** It probably would be a good idea to supplement it if indeed you are going to find yourself at the pointy end of potentially some adverse regulatory findings.

**JB** A regulator is going to be acutely conscious of not being perceived as gone soft on a corporation when there are public health issues at stake?

**AG** Once you've moved beyond that initial response phase where the priority is providing assistance to the regulator or the authorities at the time, you then move more into a longer term investigative phase and that can go on for many months or many years. Individuals need to be prepared for that so I think you move more into preparing employees for how they may participate in an interview with a regulator, getting more documentation and doing further reviews, root cause reviews and the like into what's occurred. Various stakeholders, including your board are going to want some assurances pretty quickly - to understand what's occurred, why it's occurred and what's being done to prevent it from occurring again. That can be a double edged sword sometimes because it obviously shows there is a problem in the first place but that always seems like a no-brainer to me, you just need to get on the front foot and address it.

## Prior planning prevents...

**JB** Back to your opening example Andy - an incident that happens on New Year's Eve. A lot of this it seems can be improved with some scenario planning and understanding how you'd deal with this sort of thing?

**AG** A lot of our clients and other organisations have got some protocols in place but I find sometimes they don't really extend to cover all the relevant issues we've discussed today. Gabriel have you got some tips in terms of what organisations should have to be prepared?

**GM** Whether you're small, medium sized or large, the nature of your business is going to throw up potential crises - if you're an aviation business it's going to be a crash, if you've got a lot of machinery it's going to be an industrial accident. Virtually every crisis is predictable, and you should do scenario planning with all your relevant executives about once a year. You should have a plan that clearly articulates who is responsible for what, and alternates for the various people who are involved, because as Andy said, he phoned me up on New Year's Eve, I was in Dublin but we have a policy because it's our business, so we make sure that we're not both in the Northern Hemisphere you know. It's very important that companies themselves, when they're looking at their issues management, plan ensure that they have thought about things like the leave cycle to ensure that somebody senior is on the ground. You need at least one media spokesperson available within 1 or 2 hours of an incident happening.

Review your plan, at a minimum annually. If you don't have systems in place to track media sentiment and stakeholder sentiment, make sure that when the issue does arise that you understand precisely what you're dealing with, then you know to put in arrangements to rapidly get those in place should an issue arise.

*Gabriel McDowell is Executive Chairman of ResPublica, a leading Sydney-based full-service communications agency, focussed on corporate, financial, government, consumer, community and organisational communication. He and KWM's Andy Gray have worked together advising clients on managing the legal and communications challenges major incidents present.*

KING&WOOD MALLESONS
金杜律师事务所

# In Issue 4 of Next.


## Return, risk & reputation

Considerations for a net zero economy