

Australia: Digital services regulation – where to next?

Following the Australian federal election on 3 May 2025, the Albanese Government has been returned for a second term with an increased majority. This alert takes the chance to revisit recent developments in digital service regulation and look ahead to the Government's second term.

In brief

Regulation of digital services has been an area of rapid development during the first term of the Albanese Government.

Whilst the acceleration of digital services regulation in Australia can be traced back to key developments under the previous Morrison Government, such as the commencement of the ACCC Digital Platform Services Inquiry in February 2020 and the passage of the Online Safety Act in 2021, the last few years have seen significant developments in areas such as online safety, scams, competition and consumer law, misinformation/ disinformation regulation and privacy.

If the recent influx of rapidly developing, complex and highly interconnected developments targeting digital services feels overwhelming and difficult to stay across, then this alert is aimed at helping you to pause and take stock of recent developments, and the likely direction of travel in the latter part of 2025 following the re-election of the Albanese Government in Australia and the swearing in of a new Minister for Communications, Hon Anika Wells MP.

Contents

Key takeaways

In more detail

- Online Safety Act statutory review
- Online Content Scheme roll-out
- Age Assurance Trial
- Social media minimum age restrictions
- Proposed new competition regime for digital platforms
- Misinformation/disinformation
- Children's Online Privacy Code
- Scams

Key takeaways

Key areas of recent focus likely to continue to impact regulatory development following the re-election of the Albanese Government in Australia include:

- **Online Safety Act statutory review.** Online safety remains one of the most rapidly evolving areas of regulation of digital services. The statutory review of the *Online Safety Act 2021* (Cth) (which reported to Government on 31 October 2024) made 67 recommendations – including, notably, the introduction of a digital duty of care - that are likely to play a role in the future development of online safety law. For more information see [here](#).
- **Online Content Scheme roll-out.** The roll-out of industry codes and standards under the Online Content Scheme (in Part 9 of the Online Safety Act) started in 2021, and is ongoing - most recently with draft Phase 2 industry codes of practice currently being finalised for potential registration by the eSafety Commissioner. If any of the Phase 2 industry codes are rejected, it is likely that the eSafety Commissioner will move to make Phase 2 industry standards. The approach taken is interconnected with, and has the potential to be impacted by, possible outcomes of the Online Safety Act statutory review, as well as possible outcomes of both the Age Assurance Trial and the implementation of the Social Media minimum age restrictions mentioned below. For more information see [here](#).
- **Age Assurance Trial.** Much of the focus of the draft Phase 2 industry codes is on the protection of children from age-inappropriate content, including through the use of methods of age assurance. In parallel with this, the Australian Government has commissioned a trial of age assurance technologies. For more information see [here](#).
- **Social Media minimum age restrictions.** The Online Safety Act was revised in late 2024 to establish a mandatory minimum age of 16 years for social media use. This change provided for a 12 month implementation period (until late 2025). For more information see [here](#).

- **Proposed new competition regime for digital platforms.** On 2 December 2024 the Australian Treasury released a proposal outlining a new digital competition regime aimed at promoting competition in digital platform markets. For more information see [here](#).
- **Misinformation/disinformation.** The *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024 (Cth)* aimed at managing misinformation risks, was withdrawn due to Senate opposition. The Government announced that it would not proceed with the Bill whilst highlighting the need to improve safeguards. For more information see [here](#).
- **Children's Online Privacy Code.** The *Privacy Act 1998 (Cth)* was amended in December 2024 to introduce a number of new privacy measures, including a tort for serious invasions of privacy and a Children's Online Privacy Code. For more information see [here](#).
- **Scams.** The *Competition and Consumer Act 2010 (Cth)* was amended by the *Scams Prevention Framework Act 2025 (Cth)* in February 2025 to introduce the Scams Prevention Framework (**SPF**). The SPF reforms include a focus on digital platform providers and requires certain providers to comply with SPF principles and mandatory industry codes to protect individuals from scams. You can read more about the broader reforms in our previous alert about the Scam Prevention Framework consultation [here](#). For more information on the effects for digital platform providers see [here](#).

In more detail

Online Safety Act statutory review

The *Online Safety Act 2021 (Cth)* (**OSA**) requires a statutory independent review (**Statutory Review**) of the operation of the OSA within 3 years of its commencement.

This Statutory Review was brought forward and Ms Delia Rickard PSM was appointed to conduct the review and report to the Minister for Communications. You can read our previous alert on the Statutory Review [here](#). The **final Report** of the Statutory Review of the *Online Safety Act 2021 (Report)* was ultimately presented to the Minister on 31 October 2024, before being tabled in Parliament on 4 February 2025.

Recommendations

The Report made 67 recommendations in total. Some of the key recommendations included:

- **Digital duty of care (Recommendation 4 to 7, 39):** The introduction of a new overarching duty of care was recommended.
 - a. This would require due diligence, and be underpinned by safety by design principles, risk assessment and mitigation measures (Rec 4 and Rec 6).
 - b. Key harms that would be identified for particular attention under a duty of care would broadly include:
 - i. harms to young people
 - ii. harms to mental and physical wellbeing
 - iii. instruction or promotion of harmful practices
 - iv. threats to national security and social cohesion, and
 - v. other illegal content, conduct and activity (Rec 5).
 - c. Repeated non-compliance by services in removing content would be considered when assessing non-compliance with the duty of care (Rec 39).
 - d. Services used by more than 10 percent of the Australian population would automatically be placed in the highest risk tier and have "additional mandatory responsibilities" (Rec 7).
- **Codes (Recommendation 9):** The Report recommended empowering eSafety to create mandatory codes setting out rules on how entities can fulfil aspects of their duty of care requirements. These would not constitute safe harbours. Transitional arrangements were proposed to maintain continuity of protection under the current OSA codes and standards as new frameworks are implemented.

- **Decoupling OSA from National Classification Scheme (Recommendations 29 to 33):** The Report recommends decoupling the OSA from the National Classification Scheme, which would require class 1 and class 2 material definitions and thresholds.
- **eSafety Commission Structure (Recommendations 59 to 61):** The Report proposed moving from a single eSafety Commissioner to a "Commission" structure with a multi-member team made up of a Chair, Deputy Chair and a Commissioner, with flexibility to grow.
- **Uplift and expansion of potential penalties and enforcement (Recommendations 34, 35, 41 to 47):** The Report recommended that maximum civil penalty that court can impose be increased to the greater of 5% of global annual turnover or A\$50 million (Rec 34). Amendments to the OSA in late 2024 increased maximum penalties for non-compliance with industry codes and standards to A\$49.5 million for companies (i.e., 150,000 penalty units). It was also recommended that civil penalties for non-compliance with removal notices be increased to a maximum of A\$10 million for companies (Rec 35). New enforcement powers were also recommended, including expanded access restriction powers and options for business disruption powers for seriously harmful non-compliance by offshore operators (Rec 41 and 42). The introduction of a licensing scheme for major services as a condition of operation was also proposed (Rec 45).
- **Cost recovery mechanism (Recommendation 64):** A cost recovery mechanism was recommended to "fund the cost of regulating industry." The details of this mechanism would be developed by the Government in consultation with industry stakeholders.
- **Simplification of industry section definitions (Recommendation 2):** The Report recommended that the eight online industry sections currently regulated by the OSA and related definitions be simplified to "better reflect online safety risks and future proof the Act." The proposed four categories were:
 - a. online platforms (services providing online interaction and online content)
 - b. online search and app distribution services (services which gate-keep access to online platforms)
 - c. online infrastructure services, and
 - d. equipment and operating system services (including manufacturers, suppliers, maintainers and installers).

This reclassification would aim to streamline regulatory approaches and enhance clarity.

- **Changes to notice and takedown powers (Recommendations 14 to 24):** Many elements of the notice and takedown schemes in the OSA would be retained under the recommendations. However, some significant changes were recommended including:
 - a. reducing some timeframes regarding removal notices (Rec 15 and 16)
 - b. amending the cyber-abuse scheme by lowering the threshold of how the ordinary reasonable person would perceive material (Rec 18)
 - c. enabling eSafety to issue removal notices for certain reposted content (Rec 19)
 - d. defining online hate material (Rec 21), and
 - e. addressing "volumetric" attacks (Rec 23 and 24).
- **Multi-stakeholder 'fusion cells' (Recommendation 28):** The report identified certain 'wicked problems' as beyond the current scope of the OSA, such as "technology-facilitated abuse" and the implications of end-to-end encryption. It recommends that the Government and the regulator should both be able to convene multi-stakeholder 'fusion cells' to analyse these problems and develop coordinated solutions.

Even before the public release of the Report, the Albanese Government had already **confirmed** its in principle approval for the introduction of a legislated digital duty of care and it is likely, following its re-election, that this and potentially a range of the other recommendations from the Final Report will proceed.

Online Content Scheme roll-out

The roll-out of mandatory codes and standards under the Online Content Scheme in Part 9 of the OSA was split into two phases at the outset, and is ongoing. A brief outline of the current status and recent developments is below. You can also see our previous alerts on the Phase 1 industry codes [here](#) and the development of the Phase 1 industry standards [here](#).

As outlined above, the final Report from the Statutory Review recommended significant changes to the OSA which could have a significant impact on the existing codes and standards. However, the Report recommended the continuation of existing codes and practices under the Online Content Scheme to ensure protection during legislative transition.

Phase 1 – class 1A and class 1B material

The Phase 1 codes and standards are already in place addressing certain sub-categories of class 1 material (referred to as class 1A and class 1B material) which covered a range of both illegal, as well as high-end harmful, content.

Six Phase 1 industry codes were **registered** by the eSafety Commissioner and mostly came into effect in December 2023. These cover providers of:

- social media services
- app distribution services
- internet search engine services (note that this code came into effect on 12 March 2024)
- hosting services, and
- internet carriage services

As well as persons who manufacture, supply, maintain or install equipment used by end-users in Australia and operating system providers.

In 2024, two additional Phase 1 industry standards were developed by the eSafety Commissioner for the broader categories of:

- relevant electronic services (covering different forms of messaging and interactive gaming services), and
- designated internet services (covering most websites and apps made available to users in Australia that do not fall within any of the other categories).

In the form of the *Online Safety (Relevant Electronic Services – Class 1A and Class 1B Material) Industry Standard 2024* and the *Online Safety (Designed Internet Services – Class 1A and Class 1B Material) Industry Standard 2024*. The Phase 1 standards came into effect in December 2024.

The Phase 1 codes and standards contain a broad range of mandatory obligations that apply to providers of most online services (and associated devices) in Australia and as such, form a significant part of the regulatory approach under the OSA alongside the Basic Online Safety Expectations (which have now been in place for a number of years).

eSafety issued updated **regulatory guidance** on the Phase 1 codes and new **regulatory guidance** on the Phase 1 standards in December 2024.

The first raft of annual reporting (for those providers subject to annual reporting obligations) under the Phase 1 codes occurred in February this year. The eSafety Commissioner issued **guidance and reporting templates** in connection with this milestone.

Phase 2 – class 1C and class 2 material

Phase 2 industry codes (covering the same eight sections of the industry covered by the Phase 1 codes and standards) have been under development since mid-2024. These are aimed at the sub-categories of class 1 and class 2 material not included in Phase 1 (namely class 1C and class 2 material – which in broad terms are categories of adult material not suitable for children). Whilst the Phase 2 codes are primarily aimed at protecting and preventing children from accessing or being exposed to class 1C and class 2 material, they are also aimed at empowering all Australian end-users with effective information, tools and options to limit access to such material.

Like the Phase 1 codes, the development of the Phase 2 industry codes has been undertaken by industry bodies and associations with significant oversight and direction from the eSafety Commissioner who ultimately has the power under the OSA to register, or reject, each code. On 1 July 2024, the eSafety Commissioner issued eight notices under section 141(1) of the OSA to industry bodies and associations representing the eight sections of the online industry requiring development of the Phase 2 codes. The eSafety Commissioner also released a **Position Paper on the Development of Phase 2 Industry Codes** under the Online Safety Act in July 2024 setting out eSafety expectations for the Phase 2 codes.

The **draft Phase 2 codes** were submitted to the eSafety Commissioner for review in February and March this year. The eSafety Commissioner will ultimately determine whether to register some or all of the Phase 2 codes, or instead move to develop Phase 2 industry standards for some sections of the industry.

Age Assurance Trial

In mid-2024, the Government announced a trial of age assurance technologies (**Age Assurance Trial**), to explore the use, effectiveness, maturity and readiness of available technologies in restricting children from viewing material such as pornography and other high-impact content. This will examine technologies that could be options for implementing age assurance and access restrictions required by the Phase 2 codes mentioned above, as well as under the social media minimum age restrictions mentioned below.

There is therefore obviously significant interconnection between the Age Assurance Trial and both of these regulatory developments, and the [Age Assurance Trial website](#) indicates that the trial is expected to "guide Government decision making". However, draft Phase 2 codes fell due for submission to the eSafety Commissioner, and the *Online Safety Amendment (Social Media Minimum Age) Act 2024* (Cth) was passed, *prior* to completion of the Age Assurance Trial (which remains ongoing).

In November 2024, it was **announced** that a consortium led by Age Check Certification Scheme (**ACCS**) had been awarded the tender to complete this trial. A number of methods of age assurance are being evaluated as part of the trial, including the following:

- age verification
- age estimation
- age inference
- parental certification or controls
- technology stack deployments
- technology readiness assessments

It is expected that final report of this trial will be submitted to the Government by the end of June 2025.

Social media minimum age restrictions

The *Online Safety Amendment (Social Media Minimum Age) Act 2024* (Cth) (**OSA Amendment Act**) passed in late 2024 adding a new Part 4A to the OSA. This imposed an obligation on providers of age-restricted social media platforms to take reasonable steps to prevent age-restricted users (i.e., those under 16) from having an account. Failure to comply with this provision may incur a civil penalty up to 150,000 penalty units for body corporates (currently A\$49.5 million).

As with a number of the other definitions of relevant sections of the industry under the OSA, there has been some uncertainty regarding which services were intended to be captured by the definition of an "age-restricted social media platform" (noting that the OSA Amendment Act makes clear that an age-restricted social media platform may be, but is not necessarily, a "social media service" as defined in the OSA – they are two separate but related concepts).

The Government made a number of statements in this regard and ultimately has proposed to make legislative rules to exempt certain services such as messaging apps, online gaming services and services with health or education as their primary purpose.

The age restriction requirements will come into effect by December this year. Details about the operation of the regime are being developed throughout 2025. See [here](#).

Proposed new competition regime for digital platforms

On 2 December 2024 the Australian Treasury released a proposal outlining a new digital competition regime aimed at promoting competition in digital platform markets. Consultation on this proposal was completed on 14 February 2025. Further consultation is expected once the laws are drafted.

The proposed digital competition regime seeks to address various matters raised by the Australian Competition and Consumer Commission (**ACCC**) in the course of its Digital Platform Services Inquiry (**DPSI**) by introducing laws and regulations which will apply to designated digital platforms.

The proposed regime does not specify exactly which businesses it would apply to. Instead, the regime proposed to stipulate a wide range of digital services (similar to the 'core platform services' stipulated in the EU's Digital Markets Act), and if businesses are caught by those categories, broad call-in powers would allow the ACCC to investigate those businesses against specific quantitative thresholds and qualitative factors to determine whether the Minister should 'designate' that business to be subject to the regime.

If implemented, the proposed regime would result in digital platforms joining a discreet list of industries with specific regulation under Australian competition law, and will no doubt result in additional compliance burden and cost for businesses in Australia.

Key elements of the proposed regime are set out below:

Scope of regime

It is proposed that the CCA would stipulate a list of digital platform services which would be regulated. Initially, the following services are proposed to be covered, similar to the categories used in the EU Digital Markets Act:

- app distribution services (app marketplace services)
- digital content aggregation platform services
- social media services
- search engine services (including general and specialised search services)
- electronic marketplace services (e.g., general online marketplace services)
- video-sharing platform services
- online private messaging services (including text messaging, audio messaging and visual messaging)
- operating systems
- web browsers
- virtual assistants
- cloud computing services
- online advertising services (including ad tech services)
- media referral services

It is proposed that the Minister could update this list from time-to-time including following advice from the ACCC. The Australian Government has identified app marketplaces, ad tech services and social media services as its initial priority segments.

Designation

The proposed regime would cast a wide net to capture a broad range of digital services providers. The ACCC would then investigate businesses within its scope, and the Minister would ultimately decide through a 'designation' process whether those businesses should be subject to the regime.

When determining which platforms would be considered for designation it is proposed that the following thresholds and factors would be applied:

1. **quantitative thresholds**, such as local and/or global service-specific revenue thresholds, and thresholds which examine the number of Australian users of the platform. This approach is similar to that used in the EU and the UK, with the relevant revenue and number of users thresholds to be adjusted to reflect the size of the Australian economy and population; and
2. if the quantitative thresholds are met, then various **qualitative factors** will be considered, such as market position in the relevant service and whether the platform holds an important position between groups of users such as between consumers and businesses.

The proposal provides that, if the first 'quantitative' thresholds are not met, then the business is unlikely to be designated.

The specific quantitative thresholds and qualitative factors are yet to be determined.

The ACCC would have the power to investigate businesses who appear to meet these thresholds then recommend to the Minister that they be 'designated' under the regime. A designation investigation could be self-initiated by the ACCC or initiated at the direction of the Minister.

Following the ACCC's investigation, which would include an opportunity for stakeholder consultation, the ACCC may recommend to the Minister that the platform be designated under the regime for a prescribed period (proposed to be five years).

Key aspects of the proposed regime

Once designated, the platform would be subject to certain broad and service-specific obligations:

- **Broad, and service-specific, obligations:** Once designated, the platform would be subject to both broad and service-specific obligations. Broad obligations would target ACCC concerns such as anti-competitive self-preferencing, anti-competitive tying, impediments to consumer switching, restrictions on interoperability that limit effective competition, unfair treatment of business users, and lack of transparency.
- **Additional enforcement powers for the ACCC:** The regime would be administered by the ACCC who would proactively monitor for compliance and would be given additional enforcement powers (for example, to compel the production of

documents and information, and to conduct examinations, in relation to the obligations and objectives of the regime). The regime would also incorporate mechanisms for the ACCC to coordinate with other global regulators.

- **Exemptions:** The proposed framework would provide for the ACCC to be able to receive exemption applications and permit conduct which may otherwise breach obligations under the regime. Exemptions may be granted on grounds of public health or public security, or if it can be established that the public benefit would outweigh the public detriment.
- **Recognition of overseas compliance:** Noting many digital platforms operate across multiple jurisdictions, it is proposed that the new regime would include a mechanism to allow for platforms to make proposals to the ACCC which describe their compliance measures in other jurisdictions and seek confirmation that those measures also achieve compliance with the Australian regime.
- **Cost recovery:** The regime may include a mechanism to recover administration costs from designated platforms via a levy or fee. Such costs may be imposed where, for example, an identifiable need for regulation arises in relation to a specific platform.
- **Flexibility:** The aim of the Australian Government is that regulations can be introduced or amended from time-to-time so that the regime could respond to specific matters or needs as they arise.

Penalties

It is proposed that non-compliance with the regime would give rise to civil penalties which align with various other contraventions of the CCA, meaning a breach by a corporation could give rise to a penalty up to the greater of (per-contravention):

- A\$50 million
- If the court can determine the value of the benefit obtained — three times the value of that benefit
- If the court cannot determine the value of the benefit obtained — 30% of the body corporate's adjusted turnover during the breach turnover period.¹

Unlike other jurisdictions, at this stage it is not proposed that the Australian regime would incorporate structural remedies, however various other types of penalties would be available (including injunctions, declarations and disqualification orders).

Misinformation/disinformation

The *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024 (Cth)* (**Misinformation Bill**) was introduced to amend the *Broadcasting Services Act 1992 (Cth)* with three key objectives:

- To empower the Australian Communications and Media Authority (**ACMA**) to require digital platform providers to manage misinformation and disinformation risks
- To increase transparency on how digital platform providers manage misinformation and disinformation
- To empower users of digital communications to identify and respond to misinformation and disinformation.

The Misinformation Bill would have granted ACMA the power to create enforceable codes of conduct or standards for digital platform providers/social media companies if self-regulation fell short.

However, the Misinformation Bill triggered considerable public debate and opposition and on 25 November 2024, the federal Government withdrew the Misinformation Bill due to opposition in the Senate, with then Communications Minister Michelle Rowland **announcing** that there was "no pathway" in the upper house for the legislation to proceed. Critics across the floor had concerns the Misinformation Bill would infringe on freedom of speech and had the potential for censorship.

The Government has not indicated a present intention to bring the Misinformation Bill back to the table, meaning it is unclear where Government efforts to combat misinformation and disinformation will be directed in its second term.

¹ For further information on the relevant penalty regime, see our earlier client alert here: [Australia: Significantly increased CCA/ACL penalties now apply – 12-month grace period for UCTs \(14 November 2022\)](#).

Children's Online Privacy Code

The *Privacy and Other Legislation Amendment Act 2024* (**Privacy Amendment Act**) received Royal Assent on 10 December 2024 and has come into effect. The Privacy Amendment Act is the first tranche of Australian privacy law reform following the Attorney-General's *Privacy Act Review Report* published in February 2023. If interested in learning more about this reform, please read our update '[Australia: Tranche 1 of New Privacy Laws commence](#)' and our guidance on what you need to know moving forward '[Australia: Australian Privacy developments - What do you need to know for 2025?](#)'.

The Privacy Amendment Act contained significant measures, including a new cause of action in tort for serious invasions of privacy. Importantly, a key addition relevant to online safety is the introduction of a mandate for the Office of the Australian Information Commissioner (**OAIC**) to develop a Children's Online Privacy Code (the **Code**). The Code will set out how the Australian Privacy Principles apply to the privacy of children and can introduce further requirements. The Code will apply to an entity where:

- they are a provider of a social media service, relevant electronic service or designated internet service as defined under the Online Safety Act;
- the service is likely to be accessed by children; and
- the entity is not a health service provider.

The Code can also specify other entities which may be bound by the Code.

The Code, once completed, is set to be registered by 10 December 2026. You can read more about the progress of the Code and planned consultation milestones [here](#).

A new criminal offence of 'doxxing' has also been introduced – that is, the intentional disclosure of an individual's personal data in a manner that is reasonably menacing or harassing. You can read more about this new offence and its commencement [here](#).

The second tranche of privacy reforms are anticipated in 2025 with the Attorney-General's Department indicating that consultations will continue on a broader spectrum of issues.

Scams

In February 2025, the *Competition and Consumer Act 2010* (Cth) was amended in by the *Scams Prevention Framework Act 2025* (Cth) to introduce the Scams Prevention Framework (**SPF**). The SPF aims to regulate specific sectors to take steps to be able to prevent scams and protect individuals and small businesses. One of the sectors that will be regulated are digital service providers, which includes providers of electronic services (including social media services) as defined in the *Online Safety Act 2021* (Cth).

Scams are defined broadly as attempts to deceive a consumer which would cause loss or harm to the consumer, such as making a payment or providing personal information to a scammer. Each regulated provider must comply with the overarching principles of the SPF (**SPF Principles**) – contravention of these principles can attract civil penalties. Under the SPF, the Minister is also able to create a mandatory industry code which sets out requirements that are specific to the regulated sector (**SPF codes**) and will contain more prescriptive requirements which underpin the SPF Principles. These codes are set to be developed and consulted upon with industry in 2025.

You can also read more about the reforms in the Australian Treasury's explainer [here](#) and in our previous alert about the Scam Prevention Framework consultation [here](#).

Thank you to Jeremy Hardy and Anita Nair for your assistance in preparing this alert.

Contact Us



Adrian Lawrence
Partner
Sydney
adrian.lawrence@bakermckenzie.com



Andrew Stewart
Partner
Sydney
andrew.stewart@bakermckenzie.com



Allison Manvell
Special Counsel
Brisbane
allison.manvell@bakermckenzie.com



Nicholas Kraegen
Senior Associate
Sydney
nicholas.kraegen@bakermckenzie.com

© 2025 Baker & McKenzie. **Ownership:** This site (Site) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms, including Baker & McKenzie LLP). Use of this site does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All information on this Site is of general comment and for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulation and practice are subject to change. The information on this Site is not offered as legal or any other advice on any particular matter, whether it be legal, procedural or otherwise. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any information provided in this Site. Baker McKenzie, the editors and the contributing authors do not guarantee the accuracy of the contents and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the contents of this Site. **Attorney Advertising:** This Site may qualify as "Attorney Advertising" requiring notice in some jurisdictions. To the extent that this Site may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. All rights reserved. The content of this Site is protected under international copyright conventions. Reproduction of the content of this Site without express written authorization is strictly prohibited.

