Submission on the Second Action Plan under the National Plan to End Violence against Women and Children 2022-2032

Minderoo Foundation

July 2026

Image credit: Stellalevi via Getty Images

Minderoo Foundation Ltd (ACN 651 422 141) as trustee for The Minderoo Foundation Trust (ABN 24819440618

Acknowledgement of Country

We acknowledge the Traditional Owners of the lands on which we meet, work and live, and pay our respects to Elders past and present. We recognise the enduring strength, resilience, and leadership of Aboriginal and Torres Strait Islander peoples, and their continuing connection to Country, culture, and community.

We acknowledge that Aboriginal and Torres Strait Islander women and children continue to experience violence at disproportionately high rates as a result of the ongoing impacts of colonisation, intergenerational trauma, and systemic inequality. We honour the leadership of Aboriginal and Torres Strait Islander women, communities, and organisations in driving solutions, sharing knowledge, and advocating for an equitable future where everyone can live free from violence.

About Minderoo Foundation

Minderoo Foundation is driven by a commitment to create a future where people and the environment we depend on can thrive. Our work focuses on strengthening communities, advancing gender equality and protecting natural ecosystems. While our approach centres on long-term systems change, when urgent challenges arise, including humanitarian crises, we act quickly through targeted impact missions. We drive change by working alongside those closest to the challenge, advocating for reform, building evidence for what works and developing solutions when none exist.

Gender inequality is one of the most pervasive forms of inequality globally, and gender-based violence (GBV) is both a driver and consequence of it. Ending violence against women and children is a theme that runs across our work in primary prevention, modern slavery, child and family supports, place-based initiatives, and emerging technology.

We welcome the opportunity to contribute to the development of the Second Action Plan under Australia's National Plan to End Violence against Women and Children 2022-2032.

This submission focuses on technology-facilitated gender-based violence (TFGBV). It draws on research commissioned by Minderoo and the expertise of our partners, and we are grateful to the partners, researchers, practitioners and advocates whose work informed it, including Digital Rights Watch, the Global Institute for Women's Leadership, the Sexual Violence Research Initiative, Tech Policy Design Institute, Women's Services Network (Wesnet), Behavioural Insights Australia, Teach Us Consent, Our Watch and the University of Technology Sydney. We acknowledge the contribution of AWO in developing the analysis of how the Digital Duty of Care (DDoC) framework should be strengthened to address TFGBV and online safety, which forms the basis of several recommendations in this submission.

As a funder, convener, and advocate, Minderoo amplifies the reach and impact of partner-led initiatives across Australia. We can test approaches that are difficult to fund through other channels, connect partners working across the continuum from prevention to response and sustain effort over the longer horizons that systems change requires. In doing so, we can support, strengthen and accelerate outcomes under the Second Action Plan.

About SafeAI

SafeAI, convened by Minderoo, brings together evidence, international Artificial Intelligence (AI) experts, civil society and decision-makers to advance a balanced approach to AI policy that protects people and enables innovation that benefits humanity. Its national track research consistently shows Australians are not opposed to innovation. They want confidence that AI is safe and well governed. Australians should not have to choose between benefiting from AI and being protected from harms. That is particularly important where AI can enable, amplify or increase the reach of GBV.

Executive Summary

Technology-facilitated gender-based violence (TFGBV) is a significant and growing challenge to Australia's efforts to end GBV in a generation. Around one in two Australian adults have experienced some form of technology-facilitated abuse (TFA) in their lifetime, and women are significantly more likely to experience it as part of a pattern of co-occurring abuse from the same perpetrator.[1] TFGBV is not a distinct category of violence but an extension of existing patterns of GBV, enabled, amplified, and perpetuated through digital technologies and increasingly co-occurring with offline harm.

Emerging technologies are intensifying these risks. AI is providing perpetrators with increasingly accessible, scalable, and low-cost tools of abuse, including the creation and dissemination of non-consensual explicit deepfakes, while also embedding and reproducing gender bias at scale. Despite this, TFGBV is not recognised as a distinct priority under the First Action Plan, and Australia lacks nationally consistent definitions and measurement, a gap the *Evidence to Action: Informing Direction for the Second Action Plan consultation paper* (Consultation Paper) acknowledges.

Ending GBV requires sustained investment across prevention, early intervention, response, and healing, commensurate with the scale of the challenge. Minderoo's partnerships and approach span the full continuum of the National Plan, but this submission focuses specifically on TFGBV. Drawing on commissioned research and the expertise of our partners, we provide targeted recommendations in an area where technology is rapidly reshaping the nature, scale, and reach of violence, and where focused national action is urgently needed.

The Second Action Plan arrives at a critical moment. Following the statutory review of the *Online Safety Act 2021 (Cth),* the Australian Government has proposed a DDoC that will require online services to proactively assess and mitigate the risks their services create. Together, these reforms present an important opportunity to strengthen Australia's response to TFGBV and close a significant policy gap but only if TFGBV is expressly in scope from the outset.

Much of what is most harmful to women and girls online falls below the illegal threshold. Coordinated harassment, pile-ons, and online misogyny cause serious harm without meeting the criminal standard, and international experience shows that frameworks limited to illegal content leave that harm unaddressed. Our recommendations seek to ensure the DDoC captures TFGBV explicitly, supported by a mandatory eSafety Code, clearer employer obligations under the positive duty and accountability measures that allow compliance to be tested.

Regulation alone will not deliver the long-term reduction in violence the National Plan seeks. Our recommendations therefore call for broader prevention efforts that address the underlying gendered drivers of violence and gender inequality more broadly. Without deliberate and proactive reform, TFGBV is likely to increase in prevalence, sophistication, and impact.

Minderoo stands ready to work alongside government, industry, civil society, and philanthropy to support this effort and welcomes the opportunity to provide further advice. Please contact our Government Relations team at gov.relations@minderoo.org.

[1] Powell, A., Flynn, A., & Hindes, S. (2022). Technology-facilitated abuse: National survey of Australian adults' experiences (Research report, 12/2022). ANROWS.

1. Summary of Recommendations

Minderoo recommends the Australian Government:

1. Recognise TFGBV as a distinct priority area in the Second Action Plan, supported by a dedicated outcomes framework, nationally consistent indicators, and a coordinated data collection and measurement approach.

2. Adopt an intersectional approach to all national responses to TFGBV, recognising that different groups experience distinct and compounding forms of harm. This should include alignment with *Our Ways – Strong Ways – Our Voices: National Aboriginal and Torres Strait Islander Plan to End Family, Domestic and Sexual Violence 2026-2036*, the *Second Action Plan under Safe and Supported: The National Framework for Protecting Australia's Children 2021-2031*, the forthcoming *National Action Plan to Combat Modern Slavery 2020-25* update, proposed reforms to the *Modern Slavery Act 2018 (Cth)* to include a duty to prevent modern slavery in supply chains, and the Support for Trafficked People Program to ensure responses are culturally safe, responsive to victim-survivors needs, and developed in partnership with affected communities.

3. Ensure the proposed DDoC framework explicitly recognises and prioritises TFGBV, requiring online services to assess, prevent and mitigate foreseeable risks associated with TFGBV, including online misogyny, coordinated harassment, child sexual abuse material, image-based abuse, and emerging forms of technology enabled gender-based harm. To effectively prioritise TFGBV, the DDoC framework should also:

a) Implement Recommendation 9 of the *Online Safety Act Review* to empower the eSafety Commissioner to use the proposed DDoC-making powers to establish a dedicated mandatory Code on TFGBV, including for high-risk online services such as dating and relationship platforms as a distinct risk category. The Code should be co-designed with TFGBV experts, organisations representing the lived experience of women and girls, victim-survivors, and impacted communities. Mitigations must be tailored and include enhanced protections and signposting for victim-survivors, trusted flagger mechanisms, and appropriate internal training on TFGBV.

b) Require digital platforms operating in Australia to be registered and reachable under Australian law. Currently, some major platforms have no local legal presence, making it difficult to enforce regulatory obligations or pursue legal remedies when things go wrong. Foreign digital platforms should be required to register under the *Corporations Act 2001 (Cth)* and appoint an Australian-based agent to receive legal notices, engage with regulators, and provide a clear point of accountability for Australian users.

c) Introduce targeted accountability measures, including dedicated TFGBV transparency reporting, independent auditing mechanisms, and researcher access to platform data.

d) Strengthen user control and transparency over algorithmically curated content, including through opt-in recommender systems, to reduce involuntary exposure to harmful, violent, and misogynistic content, particularly for young people.

4. Explicitly recognise TFGBV within the Positive Duty framework under section 47C of the *Sex Discrimination Act 1984 (Cth)* and associated guidance, ensuring employers or persons conducting a business or undertaking take reasonable and proportionate measures to prevent and respond to TFGBV occurring in connection with work, with particular attention to employees and workers whose roles require a public presence or engagement with the public. This should be supported by practical guidance on identifying and managing risks arising from online harassment, threats, stalking, doxxing, and other forms of TFGBV.

5. Support primary prevention initiatives that address the underlying drivers of GBV in online and digital settings, including approaches that promote gender equality, respectful relationships education, strengthen digital literacy, and engage men and boys to prevent GBV.

6. Recognise children and young people as a priority cohort, reflecting their heightened vulnerability to TFGBV, harmful online content, and emerging digital risks such as child sexual abuse material.

7. Prioritise children and young people's experiences of TFGBV, as a key focus area for the AI Safety Institute. The AI Safety Institute should monitor, analyse and report on emerging AI-enabled harms, including the normalisation of abusive behaviours online, exposure and use of deepfakes, child sexual abuse material, exposure and use of AI companions, and other AI-enabled harms, barriers to content removal and coordinated takedowns, and the growing role of AI chatbots in providing sexualised content.

2. Technology Facilitated Gender-Based Violence

Technology-facilitated gender-based violence (TFGBV) is a subset of TFA, which describes digitally enabled behavioural patterns involving harassment, abuse, and violence.[2] The eSafety Commissioner's guidance defines TFGBV as any form of physical or non-physical violence or abuse against a person or group because of biased or harmful beliefs about gender that occur online or through digital technology.[3] It manifests in many forms, including stalking and monitoring, coercive control, sexual harassment, image based-abuse, doxxing, threats of violence, online hate, and other forms of emerging gendered harms. In the most extreme cases, TFGBV increases the risk of modern slavery crimes, such as forced labour, debt bondage, human trafficking, and forced sexual exploitation of children.[4]

Around one in two Australian adults have experienced some form of TFA in their lifetime, with women disproportionately impacted.[5] Women are significantly more likely than men to experience sexual and image-based abuse, to be abused by a man, to experience abuse within a current or former intimate partner relationship, and to experience it as part of a pattern of co-occurring abuse from the same perpetrator. A growing number of children, both in Australia and abroad, experience technology-facilitated sexual exploitation by Australian offenders.[6] The Consultation Paper recognises that Australia is falling behind in addressing these harms and notes the absence of nationally consistent definitions and measurement approaches.

Importantly, TFGBV is not solely an online safety issue. As digital technologies become embedded in every aspect of daily life, they are increasingly used to facilitate, extend, and amplify patterns of abuse and misogyny that occur both online and offline. This makes TFGBV a mainstream gender equality and violence prevention challenge, and positions online spaces as vital settings for efforts to prevent and address violence in both contexts.

TFGBV also intersects with other forms of discrimination, such as racism, ableism, ageism, and homophobia. Aboriginal and Torres Strait Islander women, women living with disability, culturally and linguistically diverse women, gender-diverse people, and young women are among those facing a heightened risk, as are women with high profile jobs or leadership positions or those experiencing family, domestic or sexual violence.[7] Accordingly, TFGBV cannot be addressed through a single response. Effective prevention and support mechanisms must be designed with an understanding of the specific harms experienced by different groups.

The prevalence and nature of TFGBV also vary across online services. On social media platforms, recommender systems can amplify misogynistic content, coordinated harassment, and the rapid spread of intimate-image abuse. Dating apps carry distinct risks because they often share location and proximity data and are used to organise in-person meetings which can facilitate stalking, sexual offences, and coercion. [8] These also carry a high prevalence of on-platform sexual harassment including non-consensual intimate image sharing, and cyberflashing.[9]

---

[2] Koukopoulos, N., Janickyj, M., & Tanczer, L. M. (2026). *Defining and conceptualizing technology-facilitated abuse ("Tech Abuse"): Findings of a global Delphi study*. *Journal of Interpersonal Violence, 41*(1–2), 249–275. https://doi.org/10.1177/08862605241310465

[3] eSafety Commissioner. (n.d.). *Gendered violence*. Australian Government. https://www.esafety.gov.au/key-topics/gendered-violence

[4] Walk Free. (2023). "Anti-Social: Modern slavery on social media" in *2023 Global Slavery Index*. Minderoo Foundation. https://cdn.walkfree.org/content/uploads/2023/05/23135406/GSI-2023-Social-Media-Spotlight.pdf; Bennett, P., Cucos, R., & Winch, R. (2024). *New Frontiers: The use of generative artificial intelligence to facilitate trafficking in persons.* Organization for Security and Co-operation in Europe. https://cdn.osce.org/sites/default/files/f/documents/7/d/579715.pdf

[5] Powell, A., Flynn, A., & Hindes, S. (2022). Technology-facilitated abuse: National survey of Australian adults' experiences (Research report, 12/2022). ANROWS.

[6] Australian Federal Police. (2025). *41 per cent jump in online child sexual exploitation reports underscores need for whole-of-community approach*. Australian Government. https://www.afp.gov.au/news-centre/media-release/41-cent-jump-online-child-sexual-exploitation-reports-underscores-need

[7] Jankowicz., N., Gomex-Okeefe, I., Hoffman, L. & Becker, A.V. (2024). *It's Everyone's Problem: Mainstreaming Responses to Technology-Facilitated Gender-Based Violence.* Columbia SIPA Institute of Global Politics.

[8] Wolbers, H., Boxall, H., Long, C., & Gunnoo, A. (2022). *Sexual harassment, aggression and violence victimisation among mobile dating app and website users in Australia* (Research Report No. 25). Australian Institute of Criminology. https://doi.org/10.52922/rr78740

[9] Wolbers, H., Boxall, H., Long, C., & Gunnoo, A. (2022).

Image-based abuse remains one of the most prevalent and damaging forms of TFGBV, yet victim-survivors rarely access formal support. The eSafety Commissioner has reported that 11% of online Australian adults have had a nude or sexual image posted or shared without their consent, and that nearly eight in ten adults would not know where to go for help.[10] These figures point to the limits of a system that depends on victim-survivors identifying, reporting, and pursuing removal of harmful content themselves.

Technology is outpacing the frameworks designed to govern it. This reinforces the need for policy settings that anticipate and mitigate foreseeable risks rather than responding only after harm has occurred. It also presents an opportunity for the Second Action Plan to establish a coordinated whole-of-system national approach to TFGBV.

3. Response to the consultation questions

While the National Plan and proposed reforms to the *Online Safety Act 2021 (Cth)* recognise the role technology can play in facilitating harm, TFGBV was not recognised as a distinct priority within the First Action Plan. This understates the severity of TFGBV, limits the visibility of the issue, prevents a nationally consistent definition and measurement, and leaves responses fragmented across policy and service systems. The Second Action Plan can close this gap by recognising TFGBV as a national priority for a coordinated whole-of-system national approach.

This submission responds to questions in Priority Areas 1, 2 and 3, where TFGBV is most directly at issue. Delivering the changes will require coordination beyond the social services portfolio, particularly with agencies responsible for online safety and workplace protections. The Second Action Plan is well-placed to drive that alignment.

Achieving this will require sustained collaboration across government, industry, civil society, and philanthropy, informed by the expertise of victim-survivors, and the communities most affected. Minderoo is committed to playing its part.

3.1 Priority Area 1: Victim Survivors

What current or emerging issues should the Second Action Plan address, including in relation to coercive control and technology-facilitated abuse?

The Second Action Plan should recognise TFGBV as a distinct and central issue that requires sustained and coordinated national action. The Consultation Paper identifies the development of fast, effective responses to emerging forms of TFA and harm as a key opportunity. It notes that Australia lacks nationally consistent definitions and measurement approaches for TFA, limiting the ability of governments and service systems to understand the scale, nature, and impacts of these harms. International experience demonstrates that the absence of a clear definition is a genuine barrier to effective coordination, policy development, and response.[11] Emerging technologies are intensifying these risks, with rapid innovation outpacing the structures and regulations designed to guide it.

Technology is now commonly used as a tool for coercive control, surveillance, stalking, sexual harassment, image-based abuse, and intimidation in the context of domestic, family, and sexual violence. It frequently co-occurs with other forms of violence and can escalate into offline harms, including stalking, sexual violence, and physical violence.[12]

Without appropriate guardrails, AI risks reinforcing and embedding existing gender biases at scale, while emerging technologies are providing perpetrators with increasingly accessible, scalable, and low-cost tools to facilitate abuse. By breaking down language and cultural barriers, rapidly synthesising online personal data, and generating fraudulent social and professional profiles, AI is making it easier for abusers to misuse the technology to identify,

---

[10] eSafety Commissioner (2021). Impacts and needs: Image Based Abuse https://www.esafety.gov.au/research/image-based-abuse/impacts-needs

[11] Koukopoulos, N., Janickyj, M., & Tanczer, L. M. (2026). *Defining and conceptualizing technology-facilitated abuse ("Tech Abuse"): Findings of a global Delphi study*. *Journal of Interpersonal Violence, 41*(1–2), 249–275. https://doi.org/10.1177/08862605241310465

[12] Koukopoulos, N., Janickyj, M., & Tanczer, L. M. (2026).

target, and exploit victim-survivors.[13] AI now provides the tools for anyone to create highly realistic, manipulated imagery, including fake sexualised material. Currently, where safeguards exist, they are easily circumvented by bad actors in several ways, from simple natural language prompts to depict fictional events, prompt injections, jailbreak tactics, and model diversions of open-source AI models.[14]

AI-generated image-based abuse is becoming increasingly pervasive among young people,[15] and is another tactic used by perpetrators, particularly against those already at high risk of intimate partner violence and coercive control. For many victim-survivors, this forms part of a broader pattern of abuse, as the evolving technological landscape provides perpetrators with new avenues to exert control. At the same time, criminal legal frameworks struggle to keep pace with these evolving harms.

Technology is evolving rapidly, and the frameworks that govern it must evolve just as quickly to protect people most at risk of harm. The Second Action Plan should therefore adopt a proactive and prevention-focused approach that recognises TFGBV as a cross-cutting issue requiring dedicated attention across prevention, early intervention, response, and healing. It must clearly state that AI-generated image-based abuse, even where identities are distorted, is not a 'victimless' crime.[16]

Minderoo recommends that the Second Action Plan explicitly recognise TFGBV as a distinct priority area or key setting, supported by a dedicated outcomes framework and nationally consistent indicators. This should include a nationally consistent, legislated definition of TFGBV, building on existing eSafety guidance and international evidence. It should also include a coordinated national approach to data collection, reporting, and measurement to improve understanding of prevalence, emerging risks, and the effectiveness of interventions.

Any national response to TFGBV must be grounded in and aligned with Our Ways – Strong Ways – Our Voices: National Aboriginal and Torres Strait Islander Plan to End Family, Domestic and Sexual Violence 2026-2036. This is essential to ensuring responses to TFGBV are culturally safe, community-led, and developed in partnership with Aboriginal and Torres Strait Islander communities. Similarly, the national response should align with forthcoming updates to the *Second Action Plan under Safe and Supported: The National Framework for Protecting Australia's Children 2021-2031* and the *National Action Plan to Combat Modern Slavery 2020-25,* proposed reforms to the *Modern Slavery Act 2018 (Cth*) and Support for Trafficked People Program.

In parallel, the Second Action Plan should support the development of proactive regulatory approaches that place greater responsibility on technology companies to identify, assess, and mitigate foreseeable risks, including through Safety by Design principles and the proposed DDoC, as outlined in more detail below. As emerging technologies continue to reshape how violence is perpetrated, prevention must become a central objective of Australia's response, ensuring that systems are equipped not only to respond to harm, but to prevent it from occurring in the first place.

---

[13] Levesque, J. (2025). The AI-enhanced trafficking threat: Examining the technological evolution of trafficking in persons operations with AI tools. *Journal of Human Trafficking*, 1–21. https://doi.org/10.1080/23322705.2025.2572911

[14] Levesque, J. (2025).

[15] eSafety Commissioner. (2025, June 27). *eSafety urges schools to report deepfakes as numbers double* [Media release]. Australian Government. https://www.esafety.gov.au/newsroom/media-releases/esafety-urges-schools-to-report-deepfakes-as-numbers-double

[16] Anglia Ruskin University Press Office. (2024). *Growing demand on dark web for AI abuse images*. Anglia Ruskin University. https://www.aru.ac.uk/news/growing%20demand%20on%20dark%20web%20for%20ai%20abuse%20images

Recommendations:

1. Recognise TFGBV as a distinct priority area in the Second Action Plan, supported by a dedicated outcomes framework, nationally consistent indicators, and a coordinated data collection and measurement approach.
2. Adopt an intersectional approach to all national responses to TFGBV, recognising that different groups experience distinct and compounding forms of harm. This should include alignment with *Our Ways – Strong Ways – Our Voices: National Aboriginal and Torres Strait Islander Plan to End Family, Domestic and Sexual Violence 2026-2036*, the *Second Action Plan under Safe and Supported: The National Framework for Protecting Australia's Children 2021-2031*, the forthcoming *National Action Plan to Combat Modern Slavery 2020-25* update, proposed reforms to the *Modern Slavery Act 2018 (Cth)* to include a duty to prevent modern slavery in supply chains, and the Support for Trafficked People Program to ensure responses are culturally safe, responsive to victim-survivors needs, and developed in partnership with affected communities.

3.2 Priority Area 2: Prevention and early intervention

How can existing efforts to prevent violence be strengthened or built upon at the individual, community, organisational, institutional and societal levels?

The Consultation Paper identifies key opportunities to strengthen prevention and early intervention under the Second Action Plan, including addressing the structural drivers of violence, backlash against gender equality, and the growth of online misogyny. As digital technologies become increasingly embedded in social, economic, and civic life, efforts must extend beyond individual behaviour change and victim-survivor responses to address the systems, technologies, and structures that enable harm.

Governments have a critical role in creating the conditions for prevention and early intervention through policy and legislative reform, including by strengthening accountability for technology developers and online platforms. This approach recognises that digital and online settings are not only places where harm occurs, but also important settings for primary prevention. By addressing both the design of technologies and the broader social conditions that underpin gender inequality and GBV, Australia can strengthen efforts to prevent TFGBV before it occurs.

Prioritising TFGBV under the 'DDoC' regime

A significant opportunity to strengthen prevention and early intervention efforts lies in Australia's proposed DDoC reforms to the *Online Safety Act 2021 (Cth)*. This legislation currently operates as a complaints-based removal regime, requiring victim-survivors to identify, report, and seek removal of harmful content after harm has occurred. While these mechanisms remain important, they place a substantial burden on victim-survivors.

Under the proposed DDoC's illegal content duty, online services would be required to put in place systems and processes to monitor and prevent tech-facilitated harms. However, other forms of TFGBV, such as coordinated pile-ons, harassment, and online misogyny, may not meet the illegal threshold, despite being profoundly harmful to women and girls. For this reason, the DDoC must name TFGBV and gender-based harm to mental and physical wellbeing explicitly under the general duty to 'provide a safe online environment for all Australians'. This would ensure online services adopt a gendered Safety by Design lens to the risk assessment and mitigation process to consider TFGBV harms that fall below the illegal threshold.

International experience demonstrates the consequences of leaving this gap unaddressed. The UK's Online Safety Act 2023 does not have an overarching duty of care to identify and mitigate risk from service design or functionality. Instead, it requires services to assess and mitigate risks only in relation to illegal content and content harmful to children. As a result, the UK has prioritised illegal TFGBV such as non-consensual intimate image abuse and cyberflashing, meaning services not are not required to assess or mitigate misogyny and TFGBV that falls below the illegal threshold.

The EU's Digital Services Act requires online services to operate a complaints and takedown process for unlawful content and places an overarching duty on 'Very Large Online Platforms' to assess and mitigate systemic risks, including online GBV.[17] The EU Directive to Combat Violence Against Women sets minimum standards for the criminalisation of certain forms of GBV, including non-consensual intimate image abuse and cyberstalking.[18] In June 2026, the European Council called for stronger action on cyber violence, emphasising that online platforms must pursue safety by design, moderate effectively and prevent the misuse of their services, and that trusted flaggers on GBV need to be adequately funded.[19]

Australia's DDoC should learn from international experience by ensuring TFGBV, including lawful but harmful misogyny, is expressly within scope from the outset. The DDoC framework could be complimented by requiring online services to proactively share relevant TFGBV risk indicators with public authorities, and narrower accountability models, such as a Digital Domestic Violence Order (a court-style order that would require a named platform to take specific protective steps in relation to an at-risk individual or perpetrator), supported by requirements for platforms to maintain a clear legal point of contact and accountability within Australia.

A Dedicated Code on TFGBV

Minderoo supports the Australian Government's commitment to introduce accountability mechanisms including mandatory transparency reporting, an independent audit regime, and researcher access to platform data, to enable third parties to monitor, measure, and validate online service compliance with their duty of care and identify emerging TFGBV harms.

In line with Recommendation 9 of the Report of the Statutory Review of the *Online Safety Act 2021 (Cth),* which recommends empowering the eSafety Commissioner to make mandatory codes specifying how entities can comply with certain aspects of the duty of care requirements, including addressing specific online harms, we recommend eSafety be empowered to use the proposed DDoC code-making powers to develop a dedicated mandatory Code addressing TFGBV, including for high-risk online services such as dating and relationship platforms as a distinct risk category.[20] The Code should include enforceable standards, compliance timelines, and meaningful penalties for non-compliance.[21] This Code should focus on digital services where these harms are most prevalent, including social media platforms and dating apps. eSafety should lead a public consultation on the Code to ensure it is developed through meaningful engagement with TFGBV experts, organisations representing the lived experience of women and girls, victim-survivors, and impacted communities. eSafety's long-standing focus on TFGBV and its existing industry guidance on Technology, gendered violence and Safety by Design provide a strong foundation to begin developing this Code.[22]

In practice, the Code should establish clear and enforceable requirements for how regulated services identify, assess, mitigate and respond to TFGBV risks. It should set out how services should conduct risk assessments of TFGBV harms, including consideration of patterns of abuse, repeat offenders, and cross-platform risks. It should also set out tailored mitigation strategies, systems, and processes which are expected across different online

[17] European Commission (n.d.). *The Digital Services Act*. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act

[18] European Parliament. (2024, February 6). *First ever EU rules on combating violence against women: Deal reached* [Press release]. https://www.europarl.europa.eu/news/en/press-room/20240205IPR17412/first-ever-eu-rules-on-combating-violence-against-women-deal-reached; Center for Democracy and Technology. (n.d.). *Online gender-based violence in the EU: What now?* https://cdt.org/insights/online-gender-based-violence-in-the-eu-what-now/

[19] Council of the European Union. (2026, June 29). *Safer online spaces for girls: Council calls for stronger action against cyber violence* [Press release]. https://www.consilium.europa.eu/en/press/press-releases/2026/06/29/safer-online-spaces-for-girls-council-calls-for-stronger-action-against-cyber-violence/

[20] Rickard, D. (2024). *Report of the statutory review of the Online Safety Act 2021*. Australian Government, Department of Infrastructure, Transport, Regional Development, Communications and the Arts. https://www.infrastructure.gov.au/sites/default/files/documents/report-of-the-statutory-review-of-the-online-safety-act-2021-february-2025.pdf

[21] While the scope of this submission is confined to early intervention and primary prevention of TFGBV, Minderoo notes the South Australian Government's proposal to introduce criminal penalties for serious domestic, family, sexual violence offenders who access dating platforms. This proposal is supported by online dating providers, such as Match Group. A nationally consistent approach would maximise its impact and Minderoo encourages all State and Territories to consider adopting the measure.

[22] eSafety Commissioner. (2024, September). *Technology, gendered violence and Safety by Design: An industry guide for addressing technology-facilitated gender-based violence through Safety by Design*. Australian Government. https://www.esafety.gov.au/sites/default/files/2024-09/SafetyByDesign-technology-facilitated-gender-based-violence-industry-guide.pdf

services. This should include acting on TFGBV complaints within reasonable and defined timelines, clearly documenting enforcement action, and automatically escalating certain complaints to specialist trained trust and safety teams once trigger points are met, such as credible threats of violence, stalking indicators or sexual coercion. Where a victim-survivor identifies themselves as being at risk, services should be required to provide enhanced privacy and safety protections through a rapid response system, including access to specialist trained support teams and signposted referrals to relevant services and helplines. High-risk services, such as dating and relationship platforms, should be required to implement mechanisms for cross-platform moderation to combat the risk of cross-platform harms and perpetrators. These enhanced protections, alongside existing content classification systems and user-reporting processes, should be developed and regularly reviewed in partnership with TFGBV experts, victim-survivors, and impacted communities.

The UK experience underlines why voluntary guidance alone is insufficient. Ofcom, the UK regulator, was empowered to create Guidance on Women and Girls, which sets out a combination of 'foundational' mandatory and best practice mitigation measures for TFGBV across a range of online services.[23] This is not a mandatory code which means that online services are not required to assess and mitigate risks related to online misogyny and TFGBV that do not meet the illegal threshold. This approach has been criticised by expert TFGBV organisations,[24]with a coalition publishing its own Code of Practice on violence against women and girls (VAWG), setting out a best practice approach with a strong emphasis on systemic Safety by Design, real engagement with expert and impacted communities, and user empowerment.[25] An Australian Code should be enforceable from the outset and draw on this expert-developed model.

Accountability for Foreign Digital Platforms

Currently, some major platforms have no local legal presence, making it difficult to enforce regulatory obligations or pursue legal remedies when things go wrong. Foreign digital platforms should be required to register under the *Corporations Act 2001 (Cth)* and appoint an Australian-based agent to receive legal notices, engage with regulators, and provide a clear point of accountability for Australian users.

Social media platforms that operate in Australia but are incorporated offshore routinely present enforcement difficulties. We have seen the eSafety Commissioner, in respect of X, face the practical impossibility of process serving. Litigants with damage in Australia have no local entity to sue.

This approach models existing Australian frameworks in particular, the foreign company local agent regime in the *Corporations Act 2021 (Cth)* and the appointed actuary liability framework under the *Insurance Act 1973 (Cth)* and avoids requiring the creation of a new regulatory body. The University of Sydney Centre for AI, Trust and Governance report, Australia's Right to Regulate Technology: A Proposal for Reform, together with its supplementary report Registration as an Alternative to Licensing, are annexed to this submission and provide detailed legislative and policy proposals to strengthen accountability for foreign digital platforms operating in Australia.[26]

Introduce Complementary Accountability Measures

Minderoo supports the Australian Government's proposed accountability measures, including transparency reporting, independent audit mechanisms, and researcher access to platform data. These measures are critical to monitoring compliance with the DDoC, improving understanding of TFGBV, and strengthening the evidence base for future policy and regulatory responses.

---

[23] Ofcom. (2024). *A safer life online for women and girls: Guidance*. https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/consultation-on-draft-guidance-a-safer-life-online-for-women-and-girls/statement-docs/guidance-a-safer-life-online-for-women-and-girls.pdf?v=408215

[24] End Violence Against Women Coalition. (n.d.). *New Ofcom VAWG guidance is welcome, but more is needed to tackle online abuse*. https://www.endviolenceagainstwomen.org.uk/new-ofcom-vawg-guidance-is-welcome-but-more-is-needed-to-tackle-online-abuse/

[25] End Violence Against Women Coalition. (2022, May 16). *Violence Against Women and Girls (VAWG) Code of Practice*. https://www.endviolenceagainstwomen.org.uk/wp-content/uploads/2022/05/VAWG-Code-of-Practice-16.05.22-Final.pdf

[26] Nicholls, R., & Nolan, E. (2026, February 4). *Australia's right to regulate technology: A proposal for reform*. Centre for AI, Trust and Governance, University of Sydney; Nicholls, R., & Nolan, E. (2026, March 28). *Registration as an alternative to licensing* (Supplementary report). Centre for AI, Trust and Governance, University of Sydney.

To improve consistency and comparability, transparency reporting should include a dedicated TFGBV category with standardised metrics on the prevalence of harms, enforcement actions, complaint resolution timeframes, appeals outcomes, and platform measures to address the amplification of harmful content. eSafety should be supported to develop guidance and reporting standards to ensure consistent and meaningful disclosure across services.

Minderoo also supports the proposed powers for eSafety to commission independent audits of platform compliance and facilitate secure access to platform data for authorised researchers. Researcher access to platform data is increasingly recognised internationally as an important mechanism for understanding the role of platform design, recommender systems, and emerging technologies in enabling or amplifying online harms. These measures would strengthen transparency, support evidence-informed regulation, and improve Australia's capacity to identify and respond to emerging forms of TFGBV.

Children and young people are a particularly vulnerable group, given their developing brains often mean they can be more easily misguided or manipulated. To strengthen the proposed DDoC framework, there is an opportunity to embed user control and transparency over algorithmically curated content, including through opt-in recommender systems, to reduce involuntary exposure to harmful, violent, and misogynistic content, particularly for young people. Section 3.3 of this Submission explores the specific implications of TFGBV on children and young people in more detail.

Together, these measures would support the Second Action Plan by improving visibility of TFGBV, strengthening the evidence base on emerging harms, and enabling governments, regulators and service providers to better target prevention and response efforts. Greater transparency and independent scrutiny would help ensure policies and interventions remain responsive as technologies and patterns of abuse evolve.

Recommendation:

3. Ensure the proposed DDoC framework explicitly recognises and prioritises TFGBV, requiring online services to assess, prevent and mitigate foreseeable risks associated with TFGBV, including online misogyny, coordinated harassment, child sexual abuse material, image-based abuse, and emerging forms of technology enabled gender-based harm. To effectively prioritise TFGBV, the DDoC framework should also:

a) Implement Recommendation 9 of the *Online Safety Act Review to* empower the eSafety Commissioner to use the proposed DDoC-making powers to establish a dedicated mandatory Code on TFGBV, including for high-risk online services such as dating and relationship platforms as a distinct risk category. The Code should be co-designed with TFGBV experts, organisations representing the lived experience of women and girls, victim-survivors, and impacted communities. Mitigations must be tailored and include enhanced protections and signposting for victim-survivors, trusted flagger mechanisms, and appropriate internal training on TFGBV.

b) Require digital platforms operating in Australia to be registered and reachable under Australian law. Currently, some major platforms have no local legal presence, making it difficult to enforce regulatory obligations or pursue legal remedies when things go wrong. Foreign digital platforms should be required to register under the *Corporations Act 2001 (Cth)* and appoint an Australian-based agent to receive legal notices, engage with regulators, and provide a clear point of accountability for Australian users

c) Introduce targeted accountability measures, including dedicated TFGBV transparency reporting, independent auditing mechanisms, and researcher access to platform data.

d) Strengthen user control and transparency over algorithmically curated content, including through opt-in recommender systems, to reduce involuntary exposure to harmful, violent, and misogynistic content, particularly for young people.

TFGBV and the Positive Duty Framework

TFGBV causes substantial emotional, professional, and political harm to women. In particular, women in public-facing, leadership and high-profile roles, including journalists, politicians, academics, and community advocates, face heightened risk of TFGBV due to the nature of their roles.[27] The consequences extend beyond individual mental health and sense of safety; sustained online abuse erodes women's professional participation and visibility, deters women from seeking or remaining in public leadership roles, limits political engagement, and constrains economic potential. [28] The current system places the burden of managing abuse on women themselves via reporting, reinforcing gendered labour inequities, and perpetuating a toxic digital environment. This extends beyond victim response and points to broader structural issues, weakening the diversity of Australia's public institutions and workplaces.

The Second Action Plan presents an important opportunity to recognise and respond to these harms. In doing so, it should build on existing legislation, regulatory frameworks, and institutional infrastructure, including the positive duty under the *Sex Discrimination Act 1984 (Cth)* rather than creating parallel responses.

Workplaces have a critical role in the prevention of, and response to, TFGBV. The positive duty requires employers and persons conducting a business or undertaking to take reasonable and proportionate measures to eliminate, as far as possible, sex discrimination, sexual harassment, and hostile workplace environments. [29] Where online abuse is connected to a person's work, including where public facing duties expose workers or employees to technology facilitated harassment from third parties, the positive duty is a protection requiring employers to anticipate and mitigate that risk, rather than leaving individuals to manage it alone. However, TFGBV is not explicitly addressed within the Positive Duty Framework or the Australian Human Rights Commission's compliance guidance, creating uncertainty for employers and workers about its application to TFGBV.

By explicitly recognising TFGBV within the Positive Duty framework, the Second Action Plan can strengthen employer accountability and support safer workplaces. This should include the Australian Human Rights Commission developing practical guidance for employers on preventing and responding to work-related TFGBV, particularly for workers in public-facing roles, including elected representatives, journalists, academics, community advocates, and other leaders. Guidance should clearly outline employer responsibilities and practical measures to address risks such as online harassment, threats, stalking, doxxing, coordinated abuse, and other forms of TFA connected to work. The original Respect@Work Report flagged that technology, and modern work practices contribute to underreported harassment, placing TFGBV within the Report's original intent, but it is not yet operationalised in the Guidelines.

Recommendation:

4. Explicitly recognise TFGBV within the Positive Duty framework under section 47C of the *Sex Discrimination Act 1984 (Cth)* and associated guidance, ensuring employers or persons conducting a business or undertaking take reasonable and proportionate measures to prevent and respond to TFGBV occurring in connection with work, with particular attention to employees and workers whose roles require a public presence or engagement with the public. This should be supported by practical guidance on identifying and managing risks arising from online harassment, threats, stalking, doxxing, and other forms of TFGBV.

---

[27] Koch, L., Russo Riva, M. P., & Steinert, J. I. (2025). *Technology-facilitated gender-based violence against politically active women: A systematic review of psychological and political consequences and women's coping behaviors*. *Trauma, Violence, & Abuse*. Advance online publication. https://doi.org/10.1177/15248380251343185

[28]Koch, L., Russo Riva, M. P., & Steinert, J. I. (2025).

[29] *Sex Discrimination Act 1984 (Cth)* s 47C; see also Safe Work Australia, 2022, all employers and persons conducting a business or undertaking also have a concurrent positive duty to prevent sexual harassment under work health and safety laws.

Primary Prevention

Regulation alone is unlikely to deliver the long-term reduction in violence sought under the National Plan. While strengthened laws preventing misuse are critical, they must sit alongside broader prevention efforts that address the underlying gendered drivers of violence and gender inequality more broadly.[30]

To prevent TFGBV from occurring in the first place, solutions must extend beyond an online safety paradigm and address the social and cultural conditions that drive GBV, both online and offline. While the forms and dynamics of TFGBV may be different to other forms of violence, it is often an extension of existing GBV behaviours through digital technologies.[31] As such, there is an important opportunity for the Second Action Plan to strengthen primary prevention alongside regulatory safeguards to address the gendered drivers of violence, as defined in *Change the story*. This aligns with the National Plan's prevention pillar and commitment to *'harness technology in the prevention of violence against women and children'* and recognises the growing influence of digital environments in shaping attitudes, behaviours, and social norms.

Evidence-based initiatives that promote gender equality, whole-of-school respectful relationships education, digital literacy, and promote expressions of healthy masculinity, particularly among children and young people, can help address the attitudes and behaviours that underpin GBV. There is growing focus on the experiences of boys and men and how constructions of masculinity are shaped by digital environments that influence young people's identity, sense of purpose, belonging, and attitudes towards gender. This understanding is essential to designing effective prevention strategies that address the drivers of GBV and gender inequality, including those operating in online and digital settings.

The Second Action Plan provides an opportunity to reinforce the role of primary prevention in digital settings alongside regulatory reform. Together, these approaches can help address both the technologies that enable abuse and the social and cultural conditions that allow it to occur, supporting a more comprehensive and sustainable response to TFGBV.

Case Study: Our Watch Innovation Lab

The Violence Prevention Innovation Lab is designed and led by Our Watch and supported by Minderoo with the aim to develop, test, evaluate and scale promising violence prevention approaches for specific sectors in Australia. The Violence Prevention Innovation Lab is designed and led by Our Watch and supported by Minderoo with the aim to develop, test, evaluate, and scale promising violence prevention approaches for specific sectors in Australia. The Innovation Lab examines how digital technologies can be leveraged not only to prevent harm, but also address the attitudes, behaviours, and social norms that underpin GBV.

The first round of grants funded through the Innovation Lab address the following challenge question: *"How might we support men and boys to build safe, positive and equal relationships and reject rigid and restrictive stereotypes of what it means to be a man?"*. Grantees span a range of settings and sectors, including theatre, media, fathering, young people, settlement, LGBTQIA+, and a specific stream designed to support Aboriginal Community Controlled Organisations (ACCOs) which is led by Our Watch's Aboriginal and Torres Strait Islander team. Many of these innovative projects aim to either address TFGBV or safely leverage technology and AI to enhance their approach to change.

---

[30] Our Watch. (2021). Change the Story: A Shared Framework for the Primary Prevention of Violence Against Women in Australia (2nd ed.). Melbourne: Our Watch.

[31] Centre for Elimination of Violence Against Women. (2024). Technology-Facilitated Gender-Based Violence: Insights from Across the Indo-Pacific; eSafety Commissioner. (2023). Technology-Facilitated Abuse: Family, Domestic and Sexual Violence Literature Scan.

Recommendation:

5. Support primary prevention initiatives that address the underlying drivers of GBV in online and digital settings, including approaches that promote gender equality, respectful relationships education, strengthen digital literacy, and engage men and boys to prevent GBV.

3.3 Priority Area 3: Children and young people in their own right

How should the Second Action Plan respond to current or emerging forms of harm affecting children and young people, including technology-facilitated abuse, harmful online content, and

Minderoo supports the Consultation Paper's recognition of children and young people as victim-survivors in their own right. The Second Action Plan should apply that principle consistently across digital and physical settings – a principle that also shapes our work on early childhood development and on transitional housing for families affected by family and domestic violence.[32] Our response to this question focuses on the digital environment, where the pace of technological change is outstripping the protections available to children and young people.

The Consultation Paper identifies key opportunities to tackle emerging forms of sexual violence prevalent among young people, including concerning or harmful behaviours on dating apps, deepfakes, non-fatal strangulation, exposure to violent pornography, indoctrination into the manosphere, and financial sexual extortion. Harmful behaviours must be targeted at the source to ensure that children and young people are less exposed to harmful online content or behaviours. It is well known that technology-facilitated sexual abuse is having a profound impact on children, whose image and personal details are more accessible to abusers and traffickers than ever before, and special efforts are needed to reshape children's digital safety and ensure laws catch up to practice.[33]

Globally, organisations warn that the rise of online GBV is deeply intertwined with the rise of digital authoritarianism and the exploitation anti-feminist narratives and policies.[34] The role that tech platforms, social media, and pornography platforms play in amplifying extreme misogynistic content and causing gender harms must be appropriately addressed through regulation and enforcement.

Children and young people are a particularly vulnerable cohort, with 73% of Gen Z social-media users having seen misogynistic content online, with 70% saying they believe misogynistic language and content is increasing.[35] On average, it takes only 23 minutes for a boy or young man to encounter misogynistic content online, regardless of viewing preferences.[36] These boys and young men are not seeking out hate, but are being fed it through content recommender algorithms designed to drive engagement. Attitudes common in the 'manosphere' content reinforce gendered power structures, harmful norms, and violence against women. In normalising these attitudes amongst boys and young men towards women and girls, algorithms are winding back hard-fought progress on gender equality.

[32] Minderoo's Early Years Partnership with the Western Australian Government works with communities where family and domestic violence and the need for men's behaviour change have been identified through Community Action Plans as local priorities. Our Terminus Project addresses the lack of transitional, wraparound housing for mothers and children affected by family and domestic violence, treating children in these settings as victim-survivors with therapeutic needs equal to or greater than those of their parents.

[33] WeProtect Global Alliance (2025). *Global Threat Assessment 2025*. WeProtect. https://www.weprotect.org/wp-content/uploads/GTA-2025_EN.pdf

[34] Center for Democracy and Technology. (n.d.). *Online gender-based violence in the EU: what now?* https://cdt.org/insights/online-gender-based-violence-in-the-eu-what-now/

[35] Dublin City University's Anti-Bullying Centre (2024). *Recommending toxicity: The role of algorithmic recommender functions on YouTube Shorts and TikTok in promoting male supremacist influencers*.

[36] Dublin City University's Anti-Bullying Centre (2024).

Significant international research demonstrates the gendered nature of harmful sexual practices displayed in some pornography, and the negative impacts that such content can have on the views and expectations of young people around sex, intimacy, and gender roles.[37] Pornography platforms use content recommender algorithms to understand past engagement on the site and continue to steer users toward increasingly extreme or non-consensual content to keep them on the site. This proceeds to normalise violent and misogynistic depictions of sex, which influences and shapes their views from a young age on what healthy intimacy looks like.

There are significant research gaps in young people's experiences of TFGBV, particularly the normalisation of abusive behaviours online, exposure and use of deepfakes, and other AI enabled harms. Deepfake pornography is one of the most prevalent forms of deepfake content being created, impacting women and girls at increasing rates.[38] These technologies, including 'nudify' apps are readily available and accessible to perpetrators.[39]

Further, there is a critical gap in the understanding of young people's usage of AI chatbots to source sexualised content and information on self-harm. Generally, chatbots are not designed to have these conversations in supportive, age-appropriate, and evidence-based ways, with links being made to self-harm and suicide.[40]

There are also gaps in understanding the intersectional impacts of TFGBV. There is a lack of research on how race, ability, and sexuality shape young people's experiences online. Governments must adopt trauma-informed, intersectional strategies, recognising that various intersecting factors amplify the impacts of TFGBV and therefore must tailor mitigations to meet the specific needs of young people.

Case Study: Teach Us Consent #FixOurFeeds campaign

Minderoo partners with Teach Us Consent, a global, youth-led organisation working to deliver systems and cultural change placing consent and respectful relationships at the heart of their work. They integrate mass digital education, policy and legislative advocacy, and meaningful partnerships in culturally significant spaces to transform norms and behaviours for all young people aged 13-25.

The #FixOurFeeds campaign calls on the Australian Government to introduce an opt-in feature for social media algorithms to bring affirmative consent to our screens and turn our feeds on and off at will. They have released an open letter to the Prime Minister which has almost 12,000 signatures, including the CEO of Minderoo, John Hartman.

Recommendations:

6. Recognise children and young people as a priority cohort, reflecting their heightened vulnerability to TFGBV, harmful online content, and emerging digital risks such as child sexual abuse material.
7. Prioritise children and young people's experiences of TFGBV, as a key focus area for the AI Safety Institute. The AI Safety Institute should monitor, analyse and report on emerging AI-enabled harms, including the normalisation of abusive behaviours online, exposure and use of deepfakes, child sexual abuse material, exposure and use of AI companions, and other AI-enabled harms, barriers to content removal and coordinated takedowns, and the growing role of AI chatbots in providing sexualised content.

[37] Our Watch, & Youth Research Collective. (2026). *Young people, online worlds and respectful relationships education: What the research tells us*. Our Watch.

[38] Deep Trace Labs (2019). *The state of deepfakes: Landscape, threats, and impact.* https://regmedia.co.uk/2019/10/08/deepfake_report.pdf

[39] eSafety Commissioner (2024). *Technology, gendered violence and Safety by Design*.

[40] eSafety Commissioner (2025). *AI chatbots and companions – risks to children and young people*.

Annexure 1

THE UNIVERSITY OF SYDNEY

Australia’s Right to Regulate Technology

A proposal for reform

Centre for AI, Trust, and Governance

4 February 2026

Key Takeaways

Digital platforms have become central to Australia's economic and social infrastructure, yet they operate largely outside the comprehensive licensing and registration frameworks that govern every other systemically important sector of the economy. This regulatory exception represents a profound anomaly in Australian administrative law and creates significant enforcement challenges for regulators, limited recourse for consumers, and a fundamental accountability deficit for businesses whose reach and impact exceed many traditional industries already subject to rigorous oversight.

The universal requirement for business registration and industry-specific licensing has been a cornerstone of Australian commercial regulation for over a century, underpinning legal enforceability, consumer protection, and public accountability across banking, telecommunications, energy, broadcasting, healthcare, and construction sectors. The absence of equivalent requirements for digital platforms undermines the coherence of Australia's regulatory architecture and leaves both markets and citizens exposed to risks that peer jurisdictions have moved decisively to address.

This is in the context of other aspects of platform regulation where there have been reforms. For example, restriction on use of social media by under-sixteens under the *Online Safety Amendment (Social Media Minimum Age) Act 2024* (Cth) and the associated *Online Safety (Age-Restricted Social Media Platforms) Rules 2025*, the News Media Bargaining Code under the *Competition and Consumer Act 2010* (Cth), and the prevention of scams in the *Scams Prevention Framework Act 2025* (Cth).

The constitutional foundations for a mandatory platform licensing regime are well established through the Commonwealth's telecommunications power, corporations power, and trade and commerce power, supplemented where relevant by the external affairs power. These heads of constitutional authority have supported the evolution of Australia's telecommunications regulatory framework and provide ample scope for extending licensing obligations to digital platforms operating in Australia or having outcomes for Australian users and markets.

The critical design challenge, as highlighted by both the Australian Competition and Consumer Commission and international regulatory experience, lies in ensuring that licensing obligations bind not merely an Australian-incorporated subsidiary but the entire suite of associated entities that control, influence, or benefit from platform operations. Legislative mechanisms requiring designation of a principal entity with statutory liability for the conduct of related corporate actors, coupled with express extraterritorial application for conduct with Australian outcomes, can remedy the jurisdictional arbitrage that has frustrated effective enforcement under existing frameworks.

International regulatory convergence demonstrates both the feasibility and necessity of platform licensing regimes. The European Union's Digital Markets Act and Digital

Services Act, the United Kingdom's Online Safety Act and Digital Markets, Competition and Consumers Act, Japan's Act on Improving Transparency and Fairness of Digital Platforms, and South Korea's telecommunications-based framework all impose mandatory registration, designation criteria for systemically significant platforms, and enforceable ex ante obligations tailored to platform power and risk. These frameworks share common features including risk-based designation thresholds, transparency obligations regarding algorithmic systems and content moderation, mandatory reporting and audit requirements, substantial financial penalties for non-compliance, and mechanisms for reaching cross-border conduct and affiliated entities. Importantly, these regulatory innovations have emerged in some of the world's most dynamic and innovative economies, undermining arguments that platform regulation is either economically harmful or technically infeasible. Australia's continued reliance on reactive, retrospective enforcement through general competition and consumer law places it increasingly out of step with international best practice.

A statutory licensing regime provides the superior framework for operationalising the emerging policy consensus around a digital duty of care. Both the Joint Select Committee on Social Media and Australian Society and the Rickard Review of the Online Safety Act have recommended the imposition of a single, overarching statutory duty of care for the wellbeing of Australian users, representing a fundamental shift from reactive content moderation to proactive systems-based safety obligations. However, a duty of care remains an abstract legal principle until connected to a tangible regulatory framework capable of monitoring compliance and imposing meaningful sanctions. A licensing model transforms this duty into enforceable licence conditions, creating a continuous relationship of regulatory supervision rather than episodic enforcement actions. Precedents in financial services licensing and broadcasting regulation demonstrate how licensing serves as a charter of accountability, with conditions encompassing risk assessment, adequate resources and systems, transparency and reporting, human review and redress mechanisms, and ongoing fitness-to-hold-a-licence standards.

The current regulatory vacuum is not accidental but can be traced to the pace of innovation, the global operations of platform business groups, and the historical focus of telecommunications and broadcasting law on traditional infrastructure. As a result, platforms have exploited corporate and contractual complexity, deploying multi-entity structures, offshore domicile, and ambiguous boundaries between content hosting, service provision, and commercial facilitation, to shield the global business from effective Australian oversight. Enforcement agencies have repeatedly faced defendants who argue that the relevant conduct or control lies outside Australia, or that no Australian-facing entity can be properly joined for liability, especially for conduct arising from algorithms or cross-border information flow. Determining the veracity of these arguments requires significant time from the publicly funded court system. Examples include the Office of the Australian Information Commissioner actions in respect of Meta and Cambridge Analytica, where the harm occurred in 2015 and the settlement in 2024; *Valve Corporation v Australian Competition and Consumer Commission* ([2017] FCAFC 224 on appeal from *Australian Competition and Consumer Commission v Valve Corporation* [2016] FCA 1584;[2016] FCA 1553;

and [2016] FCA 196.); and *Epic Games, Inc v Apple Inc* [2025] FCA 900, *Epic Games, Inc v Google LLC* [2025] FCA 901, and *Anthony v Apple Inc* [2025] FCA 902.

The introduction of a platform licensing regime represents not merely a technical regulatory adjustment but the formalisation of a new social licence for the digital age.

Years of platform self-regulation have been comprehensively described by parliamentary inquiry as a failed experiment, producing persistent harms, erosion of public trust, and a fundamental misalignment between the scale of platform power and the adequacy of accountability mechanisms. A licensing framework addresses these deficiencies through multiple channels including creating legal enforceability by establishing a direct regulatory relationship with designated platforms and their associated entities, enabling proportionate and graduated enforcement through a hierarchy of regulatory tools culminating in licence suspension or revocation, mandating proactive risk management through ongoing licence conditions rather than reactive enforcement after harm has occurred, and rebuilding public confidence through transparent, visible regulatory supervision by properly resourced authorities.

Access to the Australian market should be understood as a privilege contingent upon demonstrable commitment to user safety and legal compliance, not an unregulated entitlement. Similarly, good behaviour should be seen as a necessary requirement of access to Australian markets and consumers. The cost associated with good behaviour is business cost, not a voluntary burden which may or may not be taken up due to competitive pressure. By bringing digital platforms within the same framework of responsibility and accountability expected of all systemically important industries, a licensing regime offers a coherent pathway to effective governance in an increasingly digital society. In critical infrastructure and essential services, this responsibility and accountability is legislated as a condition of doing business. This issue is also critical in the context of Artificial Intelligence (AI) deployment.

Acknowledgements

The University of Sydney Centre for AI, Trust, and Governance would like to thank **Delia Rickard** and **Lizzie O'Shea** for reviewing a draft of this report. Any errors or omissions are the responsibility of the author.

Table of Contents

Executive Summary

This report examines the constitutional, legislative, and policy foundations for establishing a mandatory licensing regime for digital platforms operating in Australia. It situates this proposal within the broader architecture of Australian business regulation, analyses international regulatory frameworks, and explores the mechanisms through which licensing can operationalise emerging statutory duties of care. The central argument is that the current absence of platform-specific licensing represents a profound anomaly in Australian administrative law, one that undermines enforcement, limits consumer recourse, and creates accountability deficits inconsistent with the scale and impact of platform operations.

Constitutional and Legislative Foundations

Chapter 1 establishes that the Commonwealth possesses robust constitutional authority to enact platform licensing requirements through multiple heads of power including telecommunications, corporations, trade and commerce, and where relevant, external affairs. The telecommunications power has supported the evolution of carrier and carriage service provider regulation under the *Telecommunications Act 1997*, providing a natural foundation for extending obligations to digital platforms. The corporations power enables regulation of platform entities and critically, the reaching of associated entities and related bodies corporate that form part of global platform groups. This is reinforced by the outcomes in Australia doctrine, supporting laws that target entities whose conduct has real and substantial effect within Australian jurisdiction.

The chapter analyses the proposed *Telecommunications Amendment (Enhancing Consumer Safeguards) Bill 2025*, which represents a significant step toward modern registration frameworks for carriage service providers. While this Bill creates important foundations including statutory registers, discretionary ministerial designation powers, clear application and renewal processes, and enhanced enforcement mechanisms including substantial civil penalties, it does not establish the comprehensive platform licensing regime recommended by the Australian Competition and Consumer Commission. The ACCC's Digital Platform Services Inquiry Final Report (2025) provides both blueprint and impetus for reform, recommending tailored ex ante regulatory obligations, designation of principal entities with statutory liability for associated corporate actors, mandatory registration and licensing for platforms meeting specified criteria, and integration of consumer protection, competition, and safety objectives within a unified framework.

Critical design challenges include ensuring jurisdictional reach over associated entities, avoiding constitutional overreach through proportionate designation criteria, integrating licensing with existing privacy and safety frameworks, and establishing graduated enforcement mechanisms appropriate to platform scale and risk. The ACCC emphasises that effective regulation requires moving beyond retrospective remediation to forward-looking, systemic interventions capable of addressing the speed and complexity of digital markets.

Universal Business Regulation in Australia

Chapter 2 demonstrates that licensing and registration requirements represent the norm rather than the exception across Australian commercial activity. Corporate registration under the *Corporations Act 2001* (Cth) creates foundational legal identity and ongoing compliance obligations for commercial enterprises. Industry-specific licensing administered by regulators including the Australian Prudential Regulation Authority, Australian Securities and Investments Commission, Australian Energy Regulator, Australian Communications and Media Authority, and Australian Health Practitioner Regulation Agency sets entry conditions and performance standards tailored to sectoral risk. Occupational licensing for professions including law, medicine, building, and allied health upholds standards of competence and probity at the individual practitioner level.

These universal requirements serve multiple functions including creating public records enabling identification of responsible entities, establishing transparent standards for entry and ongoing operation, enabling regulatory surveillance, discipline, and consumer redress, and supporting market confidence through verification of legitimacy and credentials. The breadth of Australian licensing is demonstrated through detailed case studies of banking and financial services, media and broadcasting, telecommunications carriers, energy markets, and construction and professional services. In every sector examined, the requirement for formal authorisation precedes market participation, creating enforceable duties of care, disclosure, and fitness to operate.

Digital platforms are an exception to this comprehensive framework. Their ability to operate without tailored licensing, despite market power and societal reach often surpassing heavily regulated industries, represents both regulatory inconsistency and enforcement failure. This exception permits evasion of industry-specific duties of care, creates diffusion of legal accountability across corporate structures, generates delays and uncertainty for complaint resolution, and produces opaqueness in market entry, operation, and exit. The chapter traces the evolution of licensing in Australian administrative and corporate law, demonstrating its role as a foundational device for sustaining responsible and competitive commerce. Extending these frameworks to digital platforms represents not innovation but necessary evolution to bring digital commerce within the same sphere of accountability as every other business operating in Australia.

International Regulatory Practice

Chapter 3 provides comprehensive analysis of platform regulation in the United States, United Kingdom, European Union, Japan, and South Korea. The international landscape reveals decisive movement from reactive, ex post competition enforcement to mandatory registration, proactive obligations, and risk-based supervision. While regulatory approaches vary in architectural detail, they share recognition that legacy techniques are inadequate for governing platform power and that forward-looking, market-shaping interventions are necessary.

The European Union has implemented the most comprehensive framework through the Digital Markets Act, which designates gatekeepers based on quantitative thresholds and market position, and the Digital Services Act, which imposes graduated obligations scaled to platform size and risk. Both instruments require mandatory registration, impose specific conduct obligations including interoperability and data portability, mandate transparency regarding algorithmic systems and content moderation, establish substantial financial penalties up to 10 percent of global turnover, and provide mechanisms for holding parent companies jointly liable for non-compliance. The United Kingdom's approach through the Online Safety Act and Digital Markets, Competition and Consumers Act similarly combines registration requirements with risk-based codes of practice, tailored conduct obligations for designated platforms, and supervision by established regulators including Ofcom and the Competition and Markets Authority.

Japan and South Korea have anchored platform regulation within telecommunications frameworks, requiring registration of digital platform businesses, designating specified platforms for enhanced transparency obligations, mandating local representatives for offshore providers, and establishing ongoing reporting and compliance monitoring. These Asian frameworks demonstrate that effective platform governance need not await comprehensive new institutional arrangements but can build upon existing regulatory infrastructure and expertise.

Common features across jurisdictions include risk-based designation using quantitative and qualitative criteria, registration and disclosure requirements as conditions of market operation, transparency obligations regarding platform operations and algorithmic systems, extraterritorial application and liability for associated entities, and graduated enforcement mechanisms including structural remedies and market exclusion. Significantly, these frameworks have emerged in dynamic, innovative economies without preventing platform growth or technological development. Rather, they have created more contestable markets, better-protected users, and more accountable corporate conduct. For Australia, the lesson is clear. The absence of mandatory platform licensing leaves markets and consumers exposed to risks that peer jurisdictions have addressed, and patchwork existing laws lack the coherence and ex ante orientation necessary for effective governance.

Licensing as Mechanism for Enforcement

Chapter 4 demonstrates that platform licensing can serve as an effective accountability mechanism only if several structural prerequisites are satisfied.

First, licensing or registration must operate as a genuine prerequisite for lawful operation. Platforms operating without authorisation are subject to enforcement action. Second, licensing must be anchored to requirements that platforms cannot easily evade. Third, the distinction between registration and licensing in Australian law is narrower than commonly assumed. Whether the framework is formally designated as registration or licensing matters less than ensuring it operates on the principle that authorisation is mandatory and that unauthorised operation is prohibited. Fourth, infrastructure requirements modelled on broadcasting and telecommunications regulation offer practical advantages for platform governance. The key issue is to require systemically important platforms to maintain presence commensurate with their market power. Fifth, platforms must be capable of being sued and subject to Australian legal process for dispute resolution determinations to be enforceable. This necessarily means that platforms must have sufficient assets to both launch and defend legal actions, including being able to pay penalties or damages.

The path forward requires legislative clarity that registration or licensing for digital platforms of systemic significance is mandatory, not optional. In that context, licensing is conditional on demonstrating legal accountability through specified mechanisms. These elements, integrated into a coherent statutory framework, provide the foundation for effective platform governance that aligns digital commerce with the accountability standards applied across all systemically important sectors of the Australian economy.

Licensing as Mechanism for Duty of Care

Chapter 5 examines how licensing provides the superior framework for implementing statutory duties of care. Australian policy consensus has coalesced around imposing a single, overarching duty of care for user wellbeing, as recommended by both the Joint Select Committee on Social Media and Australian Society and the statutory review of the Online Safety Act. This represents a fundamental shift from reactive content moderation to proactive, systems-based safety obligations that mandate platforms design their operational architecture with safety as a core principle.

While common law negligence provides doctrinal foundations, its adversarial, corrective justice focus renders it structurally inadequate for addressing systemic algorithmic harms affecting indeterminate classes of users. Courts remain reluctant to impose liability for pure economic loss where it risks exposing defendants to unascertainable groups of claimants, making common law pathways for redress practically unviable. This necessitates statutory intervention capable of addressing systemic risk proactively rather than through reactive individual litigation.

A licensing regime translates abstract duty of care principles into concrete, enforceable obligations through several mechanisms including embedding safety requirements as licence conditions subject to regulatory monitoring, requiring ongoing risk assessment and mitigation as fitness-to-hold-a-licence standards, mandating adequate resources, systems, and governance for safety functions, establishing transparency and reporting obligations enabling regulatory supervision, and providing graduated enforcement tools culminating in licence suspension or revocation. Precedents in financial services and broadcasting demonstrate the efficacy of this model. Australian Financial Services Licences impose general obligations to act honestly and fairly, maintain competence and adequate resources, manage conflicts of interest, and have dispute resolution systems which provide mechanisms for redress. Broadcasting licences similarly impose enforceable codes regarding content standards, complaints handling, and community responsibilities.

The economic and regulatory implications of licensing extend beyond compliance mechanics. A licensing framework strengthens deterrence by introducing existential risk of market exclusion that cannot be absorbed as a cost of business, fosters proactive compliance culture by making continuous demonstration of adequate systems a condition of operation, and rebuilds public trust through transparent, robust regulatory supervision. Ultimately, platform licensing formalises a new social licence for the digital age, asserting that market access is a privilege contingent upon demonstrable commitment to user safety and legal compliance, not an unregulated entitlement.

Recommendations and Path Forward

This report supports the Australian Competition and Consumer Commission's recommendation for a tailored platform licensing regime with several key elements. First, legislative amendment to the Telecommunications Act or alternative vehicles should establish mandatory registration for all digital platforms operating in Australia or having outcomes for Australian users. Second, designation criteria based on quantitative thresholds including user numbers, revenue, and market capitalisation combined with qualitative assessment of market power, network effects, and systemic importance should identify platforms subject to enhanced licensing obligations. Third, designated platforms should be required to nominate a principal entity with statutory liability for conduct of associated corporate actors, address jurisdictional arbitrage, and create enforceable accountability.

Fourth, licence conditions should incorporate statutory duties of care including systems-based safety obligations, risk assessment and mitigation requirements, transparency regarding algorithmic systems and content moderation, human review and redress mechanisms, and adequate resources and governance for compliance. Fifth, graduated enforcement mechanisms should provide regulators with tools proportionate to breach severity including warnings and enforceable undertakings, compliance directions and remedial notices, civil penalties scaled to global revenue, and ultimately, licence suspension or revocation with market exclusion.

Integration with existing frameworks is essential. Platform licensing should complement rather than duplicate privacy regulation, online safety requirements, and competition law. Institutional arrangements should clarify regulatory roles, establish information-sharing protocols, and potentially create a Digital Platform Regulators Forum to coordinate across domains. International alignment should guide but not constrain Australian design, with regulatory cooperation agreements facilitating enforcement against cross-border platforms.

The case for platform licensing rests on multiple grounds including closing accountability gaps that undermine enforcement and limit consumer recourse, aligning digital commerce with universal business regulation standards, implementing international best practice in platform governance, and operationalising statutory duties of care through enforceable licence conditions. Years of self-regulation have proven comprehensively inadequate. The time for decisive legislative action has arrived. By establishing a licensing regime grounded in constitutional authority, informed by international experience, and tailored to Australian circumstances, Parliament can ensure that digital platforms operate within the same framework of responsibility and accountability expected of every systemically important industry, thereby protecting consumers, fostering fair competition, and maintaining Australia's digital sovereignty in an era of accelerating technological change.

Introduction

Digital platforms have fundamentally reshaped the architecture of contemporary economic and social life. Their ubiquity in mediating commerce, communication, information access, and social interaction reflects a transformation in how individuals, businesses, and governments engage with the digital environment. Yet this transformation has occurred largely outside the comprehensive regulatory frameworks that govern other systemically important sectors of the Australian economy. The result is a profound accountability deficit, one that has attracted sustained attention from parliamentary inquiries, statutory reviews, and regulatory agencies, all converging on the urgent need for reform.

In this report, the term digital platform is used to mean an online service which are distinct from networked industries. Networked industries are those which demonstrate network effects. Network effects occur when the value of a service increases as more people use it. An example is a telecommunications network, where, according to Metcalfe's Law, the value of the telecommunications network is proportional to the square of the number of users. Strictly, it is proportional to $n \times (n - 1) = n^2 - n$ for n users of a network (Shapiro and Varian, 1999). Platforms have network effects on at least two 'sides' of a market. For example, Google provides search services at no charge to users, provided that they tolerate advertising. Google sells advertising inventory to businesses that offer products aligned with the search term. There are network effects for both users and businesses (See, generally, Evans and Schmalensee 2016). This is slightly narrower than the EU approach where the Digital Services Act defines an online platform as a provider of a hosting service that, at the request of a user, stores and disseminates information to the public.

This report examines the case for establishing a mandatory licensing regime for digital platforms operating in Australia. It does so through four interconnected inquiries. First, it analyses the constitutional and legislative foundations that would support such a regime, demonstrating that the Commonwealth possesses robust authority through multiple heads of power and that existing telecommunications legislation provides a natural vehicle for extension. Second, it situates platform licensing within the broader landscape of Australian business regulation, showing that universal requirements for registration and industry-specific authorisation represent the norm across banking, telecommunications, energy, broadcasting, healthcare, and professional services. Third, it examines international regulatory practice, tracing the global movement toward mandatory registration, ex ante obligations, and risk-based supervision of digital platforms. Fourth, it explores how licensing provides a superior mechanism for operationalising emerging statutory duties of care, creating enforceable accountability through continuous regulatory supervision rather than episodic enforcement actions.

The imperative for platform licensing emerges from multiple sources. The Australian Competition and Consumer Commission's Digital Platform Services Inquiry Final Report (2025) has documented persistent regulatory gaps and enforcement limitations in existing frameworks, noting that retrospective competition law remedies are too slow and too narrow for fast-moving digital markets. The Joint Select Committee on Social Media and Australian Society (2024) has described platform self-regulation as a failed experiment, calling for introduction of overarching statutory duties of care grounded in enforceable legal mechanisms. The statutory review of the Online Safety Act (Rickard, 2025) has similarly recommended a singular duty of care encompassing safety by design principles, risk assessment, and risk mitigation, requiring systems-based approaches to address the scale of online harm. In that context, review also suggested that a licensing regime would be appropriate and identified measures to tie platforms to the jurisdiction.

These Australian developments reflect broader international regulatory convergence. The European Union has implemented comprehensive frameworks through the Digital Markets Act and Digital Services Act, imposing mandatory registration, designation criteria for gatekeepers, and enforceable ex ante obligations. The United Kingdom has enacted the Online Safety Act and Digital Markets, Competition and Consumers Act, establishing risk-based codes, registration requirements, and tailored conduct obligations for designated platforms. Japan and South Korea have anchored platform regulation within telecommunications frameworks, requiring registration, designating platforms for enhanced transparency obligations, and mandating local accountability mechanisms. Across jurisdictions, the common recognition is that market forces alone cannot adequately discipline platform conduct or protect public interests, and that legacy regulatory techniques focused on reactive enforcement are structurally inadequate for governing platform power.

Australia stands increasingly as an outlier. While platforms operating in Australia are subject to general competition law, consumer protection requirements, and sector-specific safety obligations, they are not required to hold licences as conditions of market operation. This distinguishes them from every other systemically important industry, creating both practical enforcement challenges and principled concerns about regulatory coherence. Platforms can structure their corporate affairs to frustrate legal service, avoid local accountability, and deny effective redress to Australian users. They can enter and exit markets with minimal formal process or public notification. They face diffused accountability across corporate structures, making it difficult to identify responsible entities for regulatory purposes. And they operate largely free from ongoing regulatory supervision of the kind that characterises banking, telecommunications, and broadcasting sectors.

This regulatory exception is neither inevitable nor appropriate. The constitutional authority exists to require platform licensing. International precedents demonstrate both feasibility and efficacy. Australian regulatory infrastructure including the Australian Communications and Media Authority, Australian Competition and Consumer Commission, and eSafety Commissioner already possesses relevant expertise and could be adapted for platform supervision. What is required is legislative action to establish mandatory registration, designation criteria for platforms of systemic significance, licence conditions incorporating safety and transparency obligations, and graduated enforcement mechanisms including ultimately licence suspension or revocation.

A licensing regime addresses multiple deficiencies simultaneously. It creates legal enforceability by establishing direct regulatory relationships with platforms and their associated entities, ending jurisdictional arbitrage that has frustrated enforcement. It enables proportionate, graduated intervention through a hierarchy of regulatory tools, from warnings and undertakings through compliance directions to financial penalties and market exclusion. It mandates proactive risk management through ongoing licence conditions rather than reactive enforcement after harm has occurred. And it rebuilds public confidence through transparent, visible regulatory supervision by properly resourced authorities answerable to Parliament and the public.

Importantly, licensing is not punitive regulation but framework governance. It recognises that platforms provide genuine benefits to businesses and consumers, facilitating commerce, communication, and information access in ways that enhance productivity and connectivity. The objective is not to stifle innovation or prevent platform growth but to ensure that market access is accompanied by clear responsibilities for user safety, fair dealing, and legal compliance. Just as banks, telecommunications carriers, and broadcasters operate successfully within licensing frameworks, so too can digital platforms. The question is not whether licensing is compatible with a dynamic digital economy, but whether Australia will continue to tolerate a regulatory anomaly that leaves its markets and citizens less protected than those in peer jurisdictions.

This report proceeds in five chapters Chapter 1 examines constitutional foundations and legislative context, analysing the Commonwealth’s power to enact platform licensing and the evolution of telecommunications regulation as a potential vehicle for reform. Chapter 2 demonstrates that licensing and registration represent universal features of Australian business regulation, documenting requirements across multiple sectors and situating platform exceptionalism as regulatory anomaly. Chapter 3 provides comparative analysis of international regulatory regimes, distilling common features and lessons applicable to Australian circumstances. Chapter 4 examines the role of licensing and registration in enforcing laws and regulation. Chapter 5 explores how licensing operationalises statutory duties of care, using established precedents in financial services and broadcasting to demonstrate the mechanisms through which licence conditions create enforceable accountability.

The conclusion is that platform licensing represents necessary evolution rather than revolutionary change, bringing digital commerce within the framework of responsibility and accountability that has governed Australian business for generations. The constitutional authority exists. International precedent demonstrates feasibility. Australian policy consensus supports statutory duties of care. What remains is legislative action to formalise the social licence that platforms have long claimed but rarely honoured, ensuring that access to Australian markets is contingent upon demonstrated commitment to Australian laws, Australian values, and the safety and wellbeing of Australian users.

1 Chapter 1: Foundations of a Platform Licence in Australian Law

1.1 Introduction

The trajectory of Australia's legislative and regulatory response to digital platforms has reflected the broader international struggle to bring new forms of market power, network effects, and technological complexity within the remit of public accountability (Taylor, 2021). Against this backdrop, there is a pressing policy imperative for a mandatory licensing regime to anchor digital platforms (particularly those with significant reach and economic impact) within the Australian legal order.

Australian consumer, competition, and communications regulators have acknowledged the challenge posed by digital platforms' ubiquity, transnational operation, and the practical difficulties they present for traditional regulation and enforcement (ACCC, 2025, p. 42). The Digital Platform Services Inquiry Final Report (2025) notes persistent regulatory gaps and enforcement limitations in the existing legislative framework, particularly the retrospective and slow nature of competition law remedies in fast-moving digital markets. Paradoxically, while platforms exert enormous private ordering power over economic and communicative systems, their capacity to avoid direct obligations under Australian law is facilitated by the current regime of class licensing and the absence of a central, locally accountable entity. Mia Garlick of Meta gave evidence to the Joint Select Committee on Social Media and Australian Society on 28 June 2024. In her role as Regional Director, Policy Ms Garlick indicated the problem:

> *The one thing I would say is that I do think a focus on exactly who's in Australia is misunderstanding the way in which we provide support and services to people in Australia. Obviously, we have people who are working on content governance systems and integrity systems, and that will benefit Australia. Our community operations team is not based in Australia, but we have dedicated market specialists who make sure that they're understanding the issues and concerns of what's happening in Australia.*

This chapter interrogates the core constitutional and legislative architecture required for such a licensing regime. It situates the question within the scope of federal power, reviews analogous regimes, and draws explicitly on recommendations and analysis in the ACCC's recent inquiry. Consideration is given to constitutional competency, the suitability of legislative vehicles, and the design challenges associated with extending jurisdictional reach to the associated entities that comprise complex platform businesses. The broader international movement toward ex ante regulation, as the ACCC highlights, further supports the rationale for reform and is referenced throughout.

Adopting a robust, carefully tailored licensing model, as now advocated by the ACCC and supported by a growing cross-section of global comparators, stands to address enforcement failures and clarify accountability for platform conduct in the Australian digital environment (ACCC, 2025, pp. 54-57).

1.2 Constitutional Foundations for a Platform Licensing Regime

1.2.1 Section 51 Powers and Institutional Precedent

The Commonwealth's legislative competence to enact a mandatory licensing regime for digital platforms is grounded in several heads of constitutional power. Chief among these are the powers over telecommunications (s 51(v)), corporations (s 51(xx)), and trade and commerce (s 51(i)), supplemented by the external affairs power (s 51(xxix)) where international obligations may be relevant.

The telecommunications power has supported the evolution of the *Telecommunications Act 1997* (Cth), which already enables both registration and licensing of carriage service providers, notwithstanding the technological changes in network operation since the Act's inception. The ACCC final report (2025) acknowledges these provisions as the natural foundation for extending obligations to digital platforms operating in, and having outcomes for, Australia (ACCC, 2025, p. 56). In recommending a new, tailored ex ante regulatory regime, the ACCC emphasises the need for legislative tools that move beyond retrospective remediation to more forward-looking and systemic interventions.

The corporations power (s 51(xx)) further reinforces the Commonwealth's authority to regulate platform entities, and especially to reach associated entities and related bodies corporate forming part of global platform groups. This is coupled with the 'outcomes in Australia' doctrine, developed both in statute and case law, supporting laws that target entities whose conduct or failure has real and substantial effect within the Australian jurisdiction (*Mutual Pools & Staff Pty Ltd v Commonwealth* [1994] HCA 9).

The trade and commerce power provides a further constitutional hook, permitting regulatory schemes directed at economic actors and exchanges that cross state or international borders. Given that most major platforms operate transnationally and act as conduits for vast flows of economic and informational exchange, this head of power serves as a crucial backstop to the primary regulatory architecture.

There is also a potential to use national security powers. There are two approaches here. One flows from the decision by Meta to block access to "news media businesses" as part of negotiations on the News Media Bargaining Code. The effect was that access to critical medical information, at the height of the COVID19 pandemic was blocked on Facebook. Bushfire warning systems were also taken offline. This is in the context of the platform portraying itself as essential infrastructure. For example, the Facebook function to 'mark as safe' after a natural disaster. The second is to consider whether the platforms form part of critical infrastructure, in line with other essential services. In this case, the approach would be an extension of the obligations under the *Security of Critical Infrastructure Act 2018* (Cth) to digital platforms.

1.2.2 Challenges of Jurisdictional Reach

A recurrent challenge, highlighted in both legislative and regulatory commentary (see ACCC, 2025, Ch.2), is ensuring that licensing obligations bind not only the Australian-incorporated entity but also the suite of associated and parent entities controlling, influencing, or benefitting from platform operation. The ACCC, following analysis of recent European and Asian legislation, calls for a designated 'principal entity' for each platform business with statutory liability for conduct by associated corporate actors with outcomes in Australia (ACCC, 2025, p. 56). Explicit legislative drafting can remedy the shortcomings currently experienced under class licensing, whereby global companies retain Australia-facing operations but shield themselves from effective legal sanction by relying on foreign corporate group structure (Taylor, 2021).

International regulatory regimes, referenced extensively by the ACCC, including the EU's Digital Markets Act, Japan's Act on Improving Transparency and Fairness of Digital Platforms, and the UK's Digital Markets, Competition and Consumers Act, all buttress the appropriateness and constitutional safety of imposing principal liability on a locally registered licensee for the acts and omissions of a broader corporate group (ACCC, 2025, pp. 46-48).

1.2.3 Principle of Proportionality and Avoidance of Constitutional Risk

Best practice, consistently reflected in High Court jurisprudence, demands that such regulatory interventions be proportionate, clear as to scope, and tied squarely to relevant constitutional heads of power. The legislative scheme must distinguish between platforms with genuinely significant Australian market position (supported by designation criteria as now proposed by the ACCC and Treasury (ACCC, 2025, p. 56)) and those not meeting the threshold, to avoid overreach and ensure constitutional robustness.

Importantly, as the ACCC repeatedly urges, the licensing regime should be closely calibrated to cover large, critical digital platforms (using both quantitative and qualitative criteria), thereby minimising both the risk of constitutional challenge and policy overreach (ACCC, 2025, p. 57).

1.2.4 Taxation

This report does not consider the issue of tax. On reason for this is the uncertainty of the effectiveness of the OECD initiative known as BEPS 2.0 (Base Erosion and Profit Shifting). BEPS 2.0 was designed to modernise international tax rules, specifically targeting how multinational enterprises shift profits (often derived from intellectual property) to low-tax jurisdictions. The initiative is a "Two-Pillar" solution:

- Pillar One allows countries to tax a portion of the profits of the world's largest and most profitable companies (such as platforms) based on where their customers are located, rather than where the company has a physical office or its intellectual property.
- Pillar Two establishes a Global Minimum Tax of 15%. This is the primary mechanism to stop the "race to the bottom" by ensuring that if a company pays less than 15% in a tax haven, other countries can "top up" that tax to the 15% floor.

This approach was agreed to by the US in 2021, but has been repudiated by the Trump administration. US companies are carved out of the provisions.

BEPS 2.0 would potentially be implemented in respect of platforms in Australia using a licensing regime. However, in January 2026 the the US Treasury finalised the "Side-by-Side" Agreement with the OECD Inclusive Framework. This agreement effectively exempts US-headquartered multinationals from the Pillar Two global minimum tax.

1.3 Class licences and Individual licences

There are two broad ways in which an activity or thing can be licensed. One is to have an individual licence in the name of a person. Typically, the address of the licensee is recorded on the licence and on a register of licensees. The other is that persons or things with common characteristics fall into a class. A 'person' means either a natural person or a juridical person. Rather than licensing each member of a class individually, the class is licensed.

One issue with class licensing is that there is no register of those persons or things. Instead, there are rules about the common characteristics. An effect of class licensing is that the location of the members of the class is not known. It is only when the conditions of the class licence are breached that enforcement may be contemplated. Breach of a class licence occurs when the common characteristics which define the class are not met.

For example, WiFi uses radiocommunications spectrum. The unlicensed use of radiocommunications devices is prohibited under section 46 of the *Radiocommunications Act 1992* (Cth). However, the *Radiocommunications (Low Interference Potential Devices) Class Licence 2015*, provides that WiFi devices that use specific frequencies and at specific powers fall into a class. These radiocommunications device are permitted to be used under the class licence. There is no requirement for a person who operates a class licensed device to apply for a licence.

In contrast, individual licences are licences which are issued to a person. There is usually, but not always, a fee associated with the issue of a licence by a government to an individual. One very common example of an individual licence is a licence to drive a motor vehicle. In New South Wales, this is referred to as a Driver Licence. One effect of individual licensing is that the location of the licensee is known, at least at the time that the licence is issued. Many forms of individual licence require that the person licensed must update an address for service from time to time. For example, if a person in New South Wales who holds a Driver Licence changes address, they must inform the licence issuer who will provide an address update to be affixed to the back of the physical Driver Licence. The electronic form of that Driver Licence is electronically updated.

If an activity requires an individual licence, it is common for the relevant legislation to clarify that engaging in that activity without an appropriate individual licence is prohibited. For example, driving in NSW without a Driver Licence is prohibited.

For many of its activities in Australia, platforms are class licensed. That is, the relevant platform such as Meta falls into a relevant class that does not require it to hold an individual licence. The effect of this is that there is no person for a regulator to hold to account unless the platform is in breach of the relevant class licence. Even then, the class licensed entity is not often required to be able to sue or be sued.

The effect of this is demonstrated in the amendments to the *Online Safety Act 2021* (Cth) contained in the *Online Safety Amendment (Social Media Minimum Age) 2024* (Cth). The amendments included a new section 63C of the *Online Safety Act 2021* (Cth) was required to define an “age-restricted social media platform”. If the platform had been individually licensed, the requirements would identify relevant licensees.

1.4 Legislative Context: The Telecommunications Act and Related Statutes

1.4.1 The Evolution of Licensing and Registration in Australian Telecommunications Law

Australia’s approach to regulating entities that control essential communications infrastructure has evolved in parallel with global trends, embracing both class and individual licensing regimes as legislative tools for market accountability. The *Telecommunications Act 1997* (Cth) established a distinction between carriers (requiring individual licences) and carriage service providers (CSPs), which have generally operated under class licences, subject to registration requirements and code-based compliance (*Telecommunications Act 1997*; *Telecommunications Amendment (Enhancing Consumer Safeguards) Bill 2025*, Schedule 1).

Recent regulatory developments reflect mounting consensus that class licensing and weak registration frameworks are ill-suited to supervise the rapidly expanding, vertically integrated platform businesses that now dominate markets for communications, commerce, and content delivery (ACCC, 2025, pp. 38-40). The proposed *Telecommunications Amendment (Enhancing Consumer Safeguards) Bill 2025*, presently before Parliament, marks a significant step toward constructing a modern registration regime for CSPs. The Bill creates a statutory register for all providers, introduces discretion for the Minister to declare classes of registrable providers, outlines clear application and renewal processes, and empowers the ACMA to impose conditions on registration and, as a last resort, to exclude non-compliant providers from the market (*Telecommunications Amendment (Enhancing*

Consumer Safeguards) Bill 2025, Schedule 1; Explanatory Memorandum, pp. 5-9). Although its present focus is on CSPs, the legislative language and underlying policy rationale would readily accommodate explicit expansion to platform businesses, as recommended both by policy experts and the ACCC (ACCC, 2025, pp. 54-57). That is, draft legislation in the Minister's portfolio could readily be used to introduce a registration scheme. As discussed in Chapter 4, this registration would provide a practical alternative to licensing,

1.4.2 Licensing as a Tool for Market Accountability and Consumer Protection

Licensing is not a foreign concept in Australia's regulatory landscape. Across domains such as energy, banking, and broadcasting, individual licensing has served both as a tool for identifying responsible parties and as a vehicle for enforcing obligations of care, transparency, and consumer protection (Explanatory Memorandum to *Telecommunications Amendment (Enhancing Consumer Safeguards) Bill 2025* (Cth), p. 7). Legislative provision for exclusion, revocation, and post-registration obligations reflect contemporary best practice in regulatory law, ensuring that entities which pose unacceptable risk or repeatedly breach their obligations can be efficiently and proportionately removed from the market, securing consumer interests without imposing unnecessary process costs (Explanatory Memorandum to *Telecommunications Amendment (Enhancing Consumer Safeguards) Bill 2025* (Cth), p. 8).

By comparison, platforms are an anomaly. Subject to neither targeted licence, nor robust registration, nor an effective domestically enforceable code of conduct, they are able to operate in Australia with minimal direct statutory accountability for cross-border or algorithmic harms (ACCC, 2025, pp. 42, 384). The ACCC's Digital Platform Services Inquiry Final Report identifies this lacuna as a key driver of market failure, enforcement gaps, and consumer detriment. The report establishes clear legislative proposals for a new digital competition regime, including up-front obligations for designated digital platforms, enforced through mandatory codes and regulatory supervision by the ACCC and ACMA (ACCC, 2025, pp. 54, 357).

1.4.3 The ACCC's Recommendations and the Proposed Regulatory Framework

The ACCC's recommendations, endorsed in principle by the Government, advocate a comprehensive *ex ante* regulatory framework for digital platforms designated as having significant market power in Australia. This framework comprises several key elements that would be achieved through a licensing or registration system. Designated platforms would be subject to mandatory codes of conduct addressing competition, consumer protection, and safety concerns, with specific obligations tailored to the nature and scale of their operations. The regime would establish clear dispute resolution mechanisms, including both internal processes and external independent review, ensuring that consumers and businesses have effective recourse when harms occur. Transparency requirements would mandate regular reporting on key metrics, algorithms, and business practices, enabling regulatory oversight and public accountability.

The ACCC proposes a principles-based designation process, using quantitative thresholds such as revenue, user numbers, and market share, combined with qualitative factors including the platform's role in essential infrastructure, barriers to entry, and potential for consumer harm (ACCC, 2025, pp. 54-57, 357-359). This approach, modelled on international best practice from the EU, UK, and Japan, enables the regime to adapt to technological change while maintaining clear criteria for regulatory intervention. The potential for consumer harm is important as it provides that the social nature of a platform can be the basis of regulation. This contrasts with the EU where the number of users is the heart of the definition of regulated Very Large Online Platforms.

A defining virtue of the Consumer Safeguards model and the ACCC's proposed reforms is their adaptability. The Bill empowers the Minister to tailor classes and grounds for registration, ensuring responsiveness to technological and market innovation (*Telecommunications Amendment (Enhancing Consumer Safeguards) Bill 2025*, Schedule 1). Penalty and exclusion provisions align with international best practice and create an architecture ready to absorb future legislative extensions, including, crucially, the licensing of platform businesses and their associated entities. The ACCC's recommendations, endorsed in principle by the Government, reflect an international convergence on ex ante digital platform regulation and furnish the substantive backdrop for ongoing legislative reform (ACCC, 2025, pp. 38-41, 54, 357).

1.5 Essential Elements of a Platform Licensing Regime

1.5.1 Designation and Threshold Criteria

A well-designed licensing regime must include clear, objective criteria for determining which platforms fall within its scope. Drawing on the ACCC's recommendations and international precedents, the designation framework should combine quantitative and qualitative factors. Quantitative thresholds might include annual revenue generated from Australian users (for example, platforms exceeding $250 million in Australian revenue), number of active Australian users (such as platforms with more than 1 million monthly active users), or global revenue thresholds for entities with Australian operations. Qualitative factors would assess the platform's systemic importance, including its role in essential communications or commerce infrastructure, the degree of user dependency on its services, and the potential scale of consumer or competition harm arising from its conduct (ACCC, 2025, pp. 54-56).

The designation process should be transparent and subject to merits review, ensuring procedural fairness while enabling the regulator to act swiftly when necessary. Platforms approaching the threshold would receive advance notice, allowing them to prepare compliance systems and engage constructively with regulatory requirements before formal designation.

1.5.2 Registration, Compliance, and Ongoing Obligations

Upon designation, platforms would be required to register with the relevant regulator (likely the ACCC, in coordination with the ACMA), providing detailed information about their corporate structure, beneficial ownership, Australian operations, and the nature of services provided to Australian users. The registration process would establish a 'principal entity' within the corporate group, responsible for compliance with Australian law and serving as the primary point of regulatory contact (ACCC, 2025, p. 56). This principal entity would bear statutory liability for the conduct of associated entities within the platform group, addressing the current problem of regulatory arbitrage through complex corporate structures.

Ongoing obligations would be tailored to the specific risks and impacts associated with different platform types and business models. Core obligations applicable to all designated platforms would likely include clear consumer complaint handling standards (transparency, timeliness, escalation options, and access to external redress if dissatisfied), participation in an independent dispute resolution scheme (funded by the platform), regular reporting to the regulator on key operational metrics and consumer outcomes, transparency regarding algorithmic systems that affect Australian users or markets, and cooperation with regulatory investigations and information requests. Necessarily, compliance obligations associated information requests would include holding records in a form and place that make them accessible to Australian courts and regulators.

Sector-specific or conduct-specific codes could impose additional obligations on platforms engaged in particular activities or operating in sensitive domains, such as platforms that host user-generated content (content moderation standards), facilitate financial transactions (consumer protection and fraud prevention), or aggregate news content (fair dealing with news businesses).

1.5.3 Corporate Structure and Associated Entities

Platform businesses whose operations have outcomes in Australia are typically organised through complex global corporate structures, often comprising multiple entities (subsidiaries, affiliates, holding companies, infrastructure partners) that jointly provide digital platform services to Australian users and markets. This structural fragmentation is strategically leveraged to shield the platform group from unified legal responsibility under Australian law for harms or breaches occurring locally.

A licensing regime must therefore explicitly address associated entities. Following the ACCC's analysis and recommendations (ACCC, 2025, pp. 54-57), the regime should require designation of a principal entity within each platform group, impose joint and several liability across the platform group for breaches of regulatory obligations, enable the regulator to 'look through' corporate structures to identify controlling entities and beneficial owners, and establish clear rules for transfer or assignment of licences when corporate structures change. These provisions, modelled on approaches in the EU Digital Markets Act and the UK's regulatory framework, ensure that platforms cannot evade accountability through corporate engineering while preserving legitimate commercial flexibility.

1.5.4 Conditions, Monitoring, and Adaptive Regulation

Registration or licensing should be subject to conditions, both standard and specific. Standard conditions would apply to all designated platforms, reflecting baseline expectations for lawful and accountable operation. Specific conditions might be imposed where a platform's particular business model, market position, or past conduct warrants additional safeguards. The regulator would retain power to vary conditions in response to changing circumstances, technological developments, or emerging risks, subject to appropriate procedural safeguards (ACCC, 2025, p. 23).

Monitoring mechanisms are critical. The ACCC emphasises the need for proactive regulatory oversight, rather than reactive enforcement after harm has occurred. This includes mandatory regular reporting by platforms on compliance metrics, independent audits of algorithmic systems and content moderation processes (where relevant), consumer satisfaction surveys and complaint data analysis, and market studies to assess the competitive and consumer impacts of platform conduct. The regulator would have power to request additional information, conduct investigations, and publish findings to inform public discourse and policy development.

1.5.5 Breach, Remediation, and Escalating Sanctions

The licensing regime must provide for a graduated and proportionate enforcement framework. Upon detection of a breach, whether through regulatory monitoring, consumer complaints, or third-party reports, the regulator would have a hierarchy of enforcement tools available. These sanctions include informal and formal warnings, enforceable undertakings, compliance directions and remedial notices, pecuniary penalties and graduated financial sanctions, and finally, revocation of licence or market exclusion.

The Consumer Safeguards Bill replaces the ineffective two-step code enforcement process with direct enforceability. Once a breach is identified, the ACMA can act immediately, not merely after repeated non-compliance (Explanatory Memorandum to *Telecommunications Amendment (Enhancing Consumer Safeguards) Bill 2025* (Cth), Schedule 2). Civil penalty provisions are harmonised with contemporary standards in the energy, banking, and consumer sectors. The maximum penalty for breaches is set at the greater of $9.99 million, three times the benefit derived, or thirty per cent of turnover during the breach period (Explanatory Memorandum to *Telecommunications Amendment (Enhancing Consumer Safeguards) Bill 2025* (Cth), Schedule 3). However, there is a strong argument that the $9.99 million should be $50 million, consistent with the Australian Consumer Law (Schedule 2 to the *Competition and Consumer Act 2010* (Cth). These changes directly reflect recommendations from both consumer advocacy and the ACCC, aiming to ensure penalties are commensurate with actual market impact and consumer harm (ACCC, 2025, pp. 41-42).

1.5.6 Consumer Protection, Dispute Resolution, and Redress

A cornerstone of the regime is the reinforcement of consumer protection standards on all sides of the multi-sided markets, including mandatory dispute resolution and direct, timely access to independent ombudsman services. Membership in the Telecommunications Industry Ombudsman (TIO), and future digital platform-specific ombudsman arrangements, becomes a condition of registration (*Telecommunications Amendment (Enhancing Consumer Safeguards) Bill 2025*, s. 96F; ACCC, 2025, p. 22). The ACCC specifically calls for internal dispute resolution with robust standards (accessibility, timeliness, accountability, ability to escalate, and the right to a human review), paired with a statutory right to external, independent dispute resolution (ACCC, 2025, Recommendation 2).

The complaints system would need a single dispute resolution provider. The Telecommunications Industry Ombudsman (TIO) released a report entitled *Digital Platforms Complaints Insights*, on 4 December 2025. This revealed a significant rise in people approaching the TIO for help with social media issues, despite the TIO not currently having the legal power to intervene. As a result, the TIO is calling on the Australian Government to expand its jurisdiction to create a “Communications Ombudsman”. This would expand the TIOs remit to include digital platforms alongside traditional telecommunications services. The TIO would provide dispute resolution, acting as an independent, external body where consumers can appeal when a social media platform’s internal complaint process fails. The TIO argues this expansion is necessary to support other government reforms, such as the under-16 social media ban and the “digital duty of care” legislation, ensuring Australians have a clear path to redress when things go wrong.

Remedies for consumers are reinforced by the ability for the regulator to order remediation, mandate reporting on complaint outcomes, and facilitate market-switching for affected users. In major breaches or persistent failure, group action and class redress may be available, enabling systemic harms to be addressed efficiently.

1.5.7 Data Privacy: Interagency Coordination and Statutory Integration

The interface between a platform licensing regime and privacy law is vital. The *Privacy Act 1988* (Cth) already imposes detailed obligations regarding the collection, use, and disclosure of personal information, and sector-specific rules in telecommunications law reinforce those standards (*Telecommunications Amendment (Enhancing Consumer Safeguards) Bill 2025*, s. 96R; Explanatory Memorandum, s. 96R). The Consumer Safeguards Bill requires the ACMA and any contracted register service provider to comply fully with the *Privacy Act*, embedding privacy protection throughout the registration, compliance, and disclosure process (Explanatory Memorandum to *Telecommunications Amendment (Enhancing Consumer Safeguards) Bill 2025* (Cth), s. 96R).

The ACCC’s Inquiry places special emphasis on closing digital privacy loopholes, the adoption of a statutory tort for serious invasions of privacy, and effective mechanisms for regulatory information-sharing to strengthen the detection, reporting, and redress of data breaches in the platform context (ACCC, 2025, p. 25).

1.5.8 International Benchmarks and Remedial Experience

International experience reveals the limits of economy-wide competition and consumer law in addressing systemic digital platform harms. The ACCC highlights that remedies imposed through litigation are often too slow or narrow in scope, enabling dominant platforms to reconfigure their conduct and avoid effective accountability (ACCC, 2025, pp. 42, 46). The EU's Digital Markets Act and the UK's ex ante codes are cited as best practice, providing up-front obligations for designated platforms, supported by targeted monitoring, mandatory reporting, and strong compliance tools for authorities and affected parties.

Legislation must, however, be continually reviewed to address technological innovation, novel business models, and emerging risks such as generative AI. The Government's response to ACCC recommendations supports an ongoing monitoring and review role for the ACCC and a permanent, resourced Digital Platform Regulators Forum to coordinate across privacy, safety, and consumer domains (ACCC, 2025, Recommendations 5 and 6).

1.6 Conclusion

The case for a licensing regime for platform businesses in Australia rests firmly on constitutional, legislative, and policy foundations. The power to require registration and licensing is well established, and existing administrative frameworks (particularly those administered by ACMA and supported by the ACCC's broader competition remit) are capable of adaptation for the platform era. Effective regulatory reach over associated entities, the integration of consumer protection and privacy principles, and a dynamic suite of enforcement measures are all achievable through focused statutory design.

Crucially, the recommendations set out in the ACCC Digital Platform Services Inquiry Final Report offer both a blueprint and an impetus for reform. They align Australia's future digital regulation with emerging best practice, providing the mechanisms necessary for up-front platform accountability, consumer and competition protection, and legal clarity amidst the complexities of globalised digital service provision. The introduction of a licensing regime through legislative amendment would not only close existing accountability gaps but would enhance Australia's digital sovereignty and consumer welfare in an era of accelerating technological change.

1.7 References

Australian Competition and Consumer Commission. (2025). *Digital platform services inquiry: Final report*. Australian Government. https://www.accc.gov.au/

Australian Energy Regulator. (n.d.). *Energy retailer authorisations*. Retrieved October 22, 2025, from https://www.aer.gov.au/retail-markets/authorisations

Australian Prudential Regulation Authority. (n.d.). *Licensing banks and insurers*. Retrieved October 22, 2025, from https://www.apra.gov.au/licensing

Commonwealth of Australia Constitution Act. (1901).

Corporations Act 2001 (Cth).

Evans, D. S., & Schmalensee, R. (2016). *Matchmakers: The new economics of multisided platforms*. Harvard Business Review Press.

European Union. (2022). Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (*Digital Markets Act*). https://eur-lex.europa.eu/

Japan. (2021). *Act on Improving Transparency and Fairness of Digital Platforms*.

Mutual Pools & Staff Pty Ltd v Commonwealth [1994] HCA 9.

Privacy Act 1988 (Cth).

Shapiro, C. and Varian, H.R. (1999) *Information Rules: A Strategic Guide to the Network Economy*, Harvard Business School Press.

Smith, E. (2021). Corporate group liability in Australian law. *University of New South Wales Law Journal, 44*(2), 115-132.

Taylor, G. (2021). Platform regulation and constitutional authority. *Australian Law Journal, 95*(6), 423-441.

Telecommunications Act 1997 (Cth).

Telecommunications Amendment (Enhancing Consumer Safeguards) Bill 2025 (Cth).

Telecommunications Amendment (Enhancing Consumer Safeguards) Bill 2025 (Cth), Explanatory Memorandum.

United Kingdom. (2023). *Digital Markets, Competition and Consumers Act 2023*.

2 Chapter 2: Universal Regulation of Australian-Operating Businesses

2.1 Introduction

Business in Australia has, for more than a century, operated within a robust framework of registration and licensing, a system integral not only to economic activity but also to the protection of community interests and the enforceability of legal obligations. From the inception of corporate registration under early colonial Companies Acts to today's national schemes for occupational licensing, the principle is consistent. Operating in the Australian marketplace is a privilege that carries with it the duty to register, seek authorisation, or both, so that legal personality is clear, public accountability is enabled, and recourse for harm or dispute is properly available to individuals, regulators, and other businesses (Borowski, 2017).

This system is not monolithic. Rather, it adapts to context, industry, and risk. Company registration under the *Corporations Act 2001* (Cth) creates the foundational legal identity for commercial enterprise. Industry-specific licensing, such as that administered by the Australian Prudential Regulation Authority (APRA) in banking or the Australian Energy Regulator (AER) in energy markets, sets terms for entry and ongoing performance. Occupational licensing, whether for lawyers, doctors, or builders, upholds standards of competence and probity at the level of the individual. Few other regulatory traditions match Australia's in scope and sophistication, integrating national and state frameworks for businesses large and small, modern and traditional.

Indeed, this landscape of permissions is so ubiquitous as to be often invisible, a taken-for-granted substrate of commercial life. It is only when an industry lacks dedicated registration, authorisation, or formal licensing, as with the dominant digital platform businesses highlighted in Chapter 1, that the anomaly becomes palpable. This chapter will demonstrate, through statutory analysis and case studies drawn from banking, media, telecommunications, energy, construction, and health sectors, that universal regulation is the norm in Australia. The gap in platform regulation is not a product of oversight but an avoidable inconsistency, one which undermines the enforceability of law, erodes consumer recourse, and challenges the coherence of administrative and corporate responsibility (Australian Competition and Consumer Commission [ACCC], 2025).

The evolution of licensing as a regulatory instrument will be further explored, tracing its roots in Australian administrative and corporate law and examining its function in creating durable, enforceable responsibilities for businesses operating within the jurisdiction. In so doing, the chapter sets out both the legal foundations and policy imperatives for redressing the anomaly that platform businesses represent.

2.2 Corporate and Occupational Foundations of Business Licensing

The structure and stability of Australia's commercial landscape owe much to the universal requirement for business registration. The process of incorporation under the *Corporations Act 2001* (Cth), administered by the Australian Securities and Investments Commission (ASIC), represents the foundational step for enterprises seeking to engage in commerce with the rights and liabilities of legal personality (Tomasic et al., 2002). Granting an Australian Company Number (ACN) and access to an Australian Business Number (ABN) through the Australian Business Register (ABR) situates companies within a detailed compliance ecosystem. Directors and office holders are subject to ongoing statutory duties to act with care and diligence, avoid improper use of position or information, and disclose relevant interests.

In parallel, a diversity of occupational licensing regimes secure standards of qualification, ethical conduct, and public protection. Lawyers in Australia must be admitted as legal practitioners and hold practising certificates issued by state admitting authorities under relevant Legal Profession Uniform Laws. Medical practitioners must be registered with the Australian Health Practitioner Regulation Agency (AHPRA), with ongoing demonstration of competency and fit-and-proper status (Willmott, 2017). The National Registration and Accreditation Scheme for health professionals, established under the *Health Practitioner Regulation National Law Act 2009* (Qld), streamlines the licensing process nationally, setting out transparent standards for registration, investigation, and discipline.

Professional licensing operates hand-in-hand with business registration. Many trades, including building, plumbing, architecture, and civil engineering, require both company-level registrations and individual practitioner licensing. The Building Professionals Board in New South Wales, the Victorian Building Authority, and similar boards across states and territories maintain registers and issue licences to ensure compliance with codes, standards, and insurance requirements (Johnston, 2016). Occupational licensing for these fields also integrates public protection functions, notably consumer complaint resolution and practitioner discipline, at a human scale that complements sector-wide regulatory efforts.

Licensing and registration generate a public record. This enables courts and regulators to ascertain responsibility for harms, track compliance, and mandate improvements. It also supports transparency, allowing purchasers, counterparties, and the broader public to check business legitimacy and practitioner credentials with minimal effort, an important feature for both legal enforceability and market trust (Australian Securities and Investments Commission [ASIC], 2024a).

The universality of these requirements sets a clear baseline. To operate in Australia, enterprises and their people must be identifiable, accredited, and individually answerable for their conduct. This system forms the regulatory backbone of the Australian economy, ensuring that even as business models change, the means of enforceability and accountability remain robust and fit for purpose.

2.3 Industry Case Studies: The Breadth of Australian Licensing and Registration

2.3.1 Banking and Financial Services

In the financial sector, licensing is central. Banks and insurers in Australia are required to hold licences issued by the Australian Prudential Regulation Authority (APRA), complemented by Australian Financial Services Licences (AFSLs) administered by the Australian Securities and Investments Commission (ASIC). These licences impose stringent prudential and conduct standards, ranging from capital adequacy requirements to obligations for responsible lending, disclosure, and consumer redress (Australian Prudential Regulation Authority [APRA], 2024; ASIC, 2024b). Entry is conditional on meeting fit-and-proper criteria, ongoing supervision, and annual reporting. Breaches may trigger suspension, revocation, heavy penalties, or management bans.

2.3.2 Media and Broadcasting

Media is similarly regulated through the Australian Communications and Media Authority (ACMA), which licenses broadcasting services, including radio, television, and other transmission platforms, setting standards for content, advertising, and community responsibilities (Australian Communications and Media Authority [ACMA], 2024). Licence renewal is subject to continued compliance, and breaches, for example misleading advertising or inappropriate content, can lead to fines, programming restrictions, or loss of licence. Community broadcasting, subscription services, and commercial free-to-air networks are all captured by sector-specific licensing regimes.

2.3.3 Telecommunications Carriers

Telecommunications carriers operating in Australia must hold specific carrier licences under the *Telecommunications Act 1997* (Cth). Carriage service providers (CSPs) are subject to registration, as discussed in Chapter 1, and the obligations include technical standards, consumer protection, and data privacy. The Australian market for telecom service provision is tightly managed, with spectrum licences, infrastructure access permissions, and ongoing compliance audits driving sector integrity and consumer welfare.

2.3.4 Energy

Participants in energy supply, including retailers, generators, and distributors, are regulated under a sophisticated suite of licences issued by the Australian Energy Regulator (AER) and state authorities, such as the Essential Services Commission (Victoria) and the Independent Pricing and Regulatory Tribunal (NSW). Conditions for licensing include financial viability, technical competence, consumer protection arrangements, and robust complaint handling. Licensing discipline has been instrumental in expanding market competition while protecting vulnerable consumers and ensuring public interest outcomes (Australian Energy Regulator [AER], 2024).

2.3.5 Building, Construction, and Engineering

Non-tech industries such as building, architecture, and engineering are subject to some of the most detailed licensing schemes in Australia. Builders, architects, structural engineers, and other trades must be registered with state-level regulators, such as the Victorian Building Authority, NSW Fair Trading, and Queensland Building and Construction Commission (Johnston, 2016). Individual practitioners are issued licences or certificates that confirm their credentials, experience, insurance cover, and ongoing fitness to practise. Companies operating in the sector are also registered, and discipline or complaints may result in suspension, cancellation, consumer compensation, or restriction from operating. Accreditation schemes further support market transparency and public confidence.

2.3.6 Health Practitioners and People-Level Licensing

The health sector illustrates people-level licensing at its most sophisticated. The Australian Health Practitioner Regulation Agency (AHPRA), established under the *Health Practitioner Regulation National Law Act 2009* (Qld), registers doctors, nurses, dentists, psychologists, and other practitioners, each subject to annual renewal and regular assessment of their ongoing competence, ethical standards, and compliance with professional codes. This system is mirrored in the legal profession, where lawyers are admitted by state boards and must hold a current practising certificate, maintain continuing education, and abide by ethical standards and insurance requirements (Willmott, 2017).

Failure to comply results in immediate investigation, disciplinary hearings, suspension, or disqualification, demonstrating both the efficiency and the necessity of licensing mechanisms for individual accountability and consumer redress. The universality of these people-level schemes underscores the anomaly presented by large, complex platform businesses operating without equivalent sectoral licence.

2.4 Platform Businesses as the Anomaly

In the extensive and interlocking web of Australian licensing and registration requirements, platform businesses stand out as the most significant regulatory anomaly of the digital age. While nearly all traditional sectors, whether technical or manual, professional or trade, are governed by schemes that require public registration and ongoing authorisation, platform businesses that intermediate vast swathes of economic and social activity mostly escape equivalent sectoral oversight.

Most prominent digital platforms, including search engines, social media networks, app stores, and gig economy intermediaries, operate in Australia only as registered corporations, with no industry-specific licensing or registration regime. Even with local incorporation, the “directing minds” are often overseas. Regulatory action in *Australian Competition and Consumer Commission v Emma Sleep Gmbh* [2025] FCA 618 demonstrates the difficulty in proving that the directing minds are “shadow” or “de facto” directors. There is no requirement for a designated entity to hold sectoral authority analogous to that demanded of a builder, banker, or radio licensee.

Nor, critically, are there clear mechanisms under current law for the imposition of enforceable, platform-specific duties or for public exclusion or suspension in cases of systemic harm (ACCC, 2025).

This regulatory vacuum is not accidental but can be traced to the pace of innovation, the global operations of platform business groups, and the historical focus of telecommunications and broadcasting law on traditional infrastructure. As a result, platforms have exploited corporate and contractual complexity, deploying multi-entity structures, offshore domicile, and ambiguous boundaries between content hosting, service provision, and commercial facilitation, to shield the global business from effective Australian oversight. Enforcement agencies have repeatedly faced defendants who argue that the relevant conduct or control lies outside Australia, or that no Australian-facing entity can be properly joined for liability, especially for conduct arising from algorithms or cross-border information flow.

There is also an issue where there is a mismatch of regulatory resources. When Uber entered Australia, it took advantage of the differences in regulatory approaches at the local government, state, and federal levels. Regulatory “wins” were used as leverage and setbacks were not shared between the relevant regulators. In this case, the pace of innovation was less of a driver than the inability to provide a coordinated response.

The absence of licensing or sectoral registration for platforms enables several problematic outcomes. First, it permits the evasion of enforceable, industry-specific duties of care and compliance, including those directed at conduct causing consumer or competition harm. Second, it creates diffusion of legal accountability, such that no single entity is readily accessible for notices, investigations, or litigation. Third, it generates delays and uncertainty for regulators and consumers seeking to resolve complaints or obtain compensation. Fourth, it produces opaqueness in market participation, entry, and exit. Platforms can reconfigure legal personality, transfer assets, or withdraw with little formal process or public notification.

Numerous regulatory and policy reviews, including the ACCC’s Digital Platform Services Inquiry, have noted the profound incoherence this creates in the law. Where financial services, energy, health, and even media are integrated into universal licensing frameworks, the digital platform sector is an outlier, one whose power, reach, and capacity for impact far exceed many other industries already governed by such obligations.

This regulatory exception not only undermines the efficacy and deterrence of the broader licensing system, but it also produces real, concrete harms for competition, consumer welfare, and the accountability of major enterprises to the public interest. It presents an urgent challenge for administrative and legislative reform, one that goes to the heart of modern principles of responsibility, governance, and the social contract of commerce in Australia.

2.5 The Evolution and Rationale of Licensing in Administrative and Corporate Law

Licensing, in its modern Australian form, is the product of centuries of adaptation in administrative and corporate law. Its historical development reflects the growing sophistication of society's expectations for both the competence and accountability of those offering goods, services, or professional expertise.

From early forms, such as guild certification and municipal charters, licensing emerged as a tool for governments to distinguish legitimate economic actors from unqualified, rogue, or fraudulent traders. In Australia, colonial companies acts and the gradual professionalisation of fields like medicine and law extended this approach, making public authorisation central to market participation and consumer trust (Borowski, 2017; Willmott, 2017). These laws provided a public record, created standards for entry, and specified grounds for removal or discipline.

Contemporary licensing systems, administered by regulatory agencies such as ASIC, APRA, AER, ACMA, and AHPRA, perform four pivotal functions. First, they create an unequivocal legal link between an entity or individual and its public obligations, including duties of care, disclosure, and fitness to practise. Second, they enable ongoing surveillance, discipline, and consumer redress, empowering regulators to respond proportionately to risk, complaint, or breach. Third, they bolster consumer and market confidence, supplying visible credentials, transparency, and accessible records for verifying legitimacy and regulatory compliance. Fourth, they motivate the associated insurance regimes for the regulated entities to provide incentives for compliance.

In administrative law, licensing is closely linked to the principles of procedural fairness and merit review. Decisions to grant, revoke, or refuse a licence must meet standards for transparency, reasonableness, and natural justice, and are generally subject to independent review bodies, such as tribunals or ombudsmen (Johnston, 2016). This ensures that licensing functions not only as a tool of control but of protective governance.

In corporate law, licensing complements the concept of separate legal personality. Companies hold their own rights and duties. Through licensing, those duties can be tailored for sectoral risk and public interest, beyond generic company law obligations. By tying market participation to formal permission, law bridges the gap between private autonomy and public accountability.

Australia's experience demonstrates that licensing thrives where benefits, including enforceability, clarity, and consumer protection, are greatest. The lack of equivalent sectoral licensing for platform businesses starkly contrasts with this tradition, raising urgent questions about enforceable responsibility, regulatory parity, and the future of market governance. Licensing is not just a matter of regulatory paperwork but a foundational legal device for sustaining Australia's vision of responsible and competitive commerce.

2.6 Conclusion

Licensing and registration underpin the integrity and effectiveness of Australia's regulatory system, defining the conditions for entry, operation, and accountability across all major sectors. Whether the business is a bank, builder, doctor, broadcaster, or energy retailer, the requirements for formal permission and public oversight are universal, evolving to match new challenges and risks. This systemic approach provides not only the foundation for consumer trust and market confidence but also the practical means for governments to enforce standards, protect the public, and ensure recourse for harm.

Platform businesses, as this chapter has demonstrated, are the significant exception. Their ability to operate absent tailored licensing, despite market power and societal reach that often surpass more heavily regulated industries, highlights an urgent lacuna in Australia's regulatory architecture. Addressing this anomaly is not simply a matter of administrative convenience but of upholding the core principles and public outcomes that licensing and registration have safeguarded for generations. The extension of these frameworks to digital platforms is a necessary evolution, one that brings digital commerce within the same sphere of responsibility as every other business in the Australian economy.

2.7 References

Australian Communications and Media Authority. (2024). *Broadcasting services regulation*. https://www.acma.gov.au/

Australian Competition and Consumer Commission. (2025). *Digital platforms services inquiry: Final report*. Commonwealth of Australia. https://www.accc.gov.au/

Australian Energy Regulator. (2024). *Retail authorisations and exemptions*. https://www.aer.gov.au/

Australian Health Practitioner Regulation Agency. (2024). *National Registration and Accreditation Scheme*. https://www.ahpra.gov.au/

Australian Prudential Regulation Authority. (2024). *Licensing and authorisations*. https://www.apra.gov.au/

Australian Securities and Investments Commission. (2024a). *Company and business name registration*. https://www.asic.gov.au/

Australian Securities and Investments Commission. (2024b). *Australian Financial Services licensing*. https://www.asic.gov.au/

Borowski, A. (2017). Regulatory histories in the Australian professions: Lessons for reforms. *Australian Journal of Public Administration*, *76*(2), 177–188. https://doi.org/10.1111/1467-8500.12216

Corporations Act 2001 (Cth).

Health Practitioner Regulation National Law Act 2009 (Qld).

Johnston, D. (2016). *Practical administration law in Australia*. LexisNexis.

Telecommunications Act 1997 (Cth).

Tomasic, R., Bottomley, S., & McQueen, R. (2002). *Corporations law in Australia* (2nd ed.). Federation Press.

Willmott, L. (2017). Professional licensing and accountability in Australia’s health system. *Medical Law Review*, *25*(3), 381–402. https://doi.org/10.1093/medlaw/fwx024

3 Chapter 3: International Practice: Comparative Regulatory Regimes

3.1 Introduction

The extraordinary reach and complexity of digital platforms have accelerated a global re-examination of regulatory frameworks and enforcement philosophies. As platform-mediated businesses cross borders and jurisdictions with ease, governments face profound challenges. The key one is to ensure that foreign-based or multi-entity digital conglomerates comply with local law, maintain fair competition, and uphold the rights and interests of citizens and markets.

Historically, regulatory intervention in digital markets was primarily reactive. Authorities relied on general competition law, sectoral consumer protection, and occasional ex post enforcement to address harms after they arose. With the rapid escalation of platform power and their integration into everyday life, this approach proved inadequate. It has been too slow, too narrow in scope, and too easily evaded by corporate and technical ingenuity. In response, leading economies have moved toward a regime of ex ante regulation, imposing up-front obligations, mandatory registration, and, increasingly, dedicated licensing requirements for major digital platforms.

Recent years have witnessed the proliferation of statutory instruments and supervisory arrangements designed to close the enforcement gap. In the United States, federal and state authorities have begun to assert new competition and consumer protection powers, while the European Union has implemented transformative laws (the *Digital Services Act* and *Digital Markets Act*) requiring designated platforms to register, disclose, and comply with enforceable duties tailored to market power and risk (European Union, 2022a, 2022b). The United Kingdom, Japan, and South Korea have similarly adopted innovative frameworks demanding accountability, transparency, and direct regulatory oversight.

These international models do not converge in every detail. Instead, they reflect a shared recognition of the inadequacies of legacy regulatory techniques and a willingness to experiment with forward-looking, risk-based, and market-shaping approaches. For Australia, the lessons and implications of this global regulatory movement are clear. The absence of sectoral licensing and registration for platform businesses is out of step with international best practice and leaves Australian consumers, markets, and public interests exposed.

This chapter explores comparative regimes in depth, drawing on statutory analysis, enforcement experience, and regulatory philosophy in the United States, United Kingdom, European Union, Japan, and South Korea. It distils the commonalities and divergences, examines mechanisms for reaching associated entities and cross-border conduct, and situates Australia's policy options within the evolving global landscape of platform regulation.

3.2 United States

The United States has historically maintained a light-touch sectoral approach to digital platform regulation, relying on broad-based antitrust laws and agency enforcement to discipline market conduct. The Federal Trade Commission is the principal regulator, vested with authority under Section 5 of the *Federal Trade Commission Act* to prohibit 'unfair or deceptive acts or practices' in commerce (15 U.S.C. §45). The Department of Justice, alongside state attorneys general, also retains significant prosecutorial powers under the Sherman and Clayton Acts to prevent collusive, exclusionary, or monopolistic behaviour.

Over the past decade, both federal and state regulators have attempted to address perceived harms from digital platforms through enforcement actions and negotiated settlements. Notable cases include *United States v Google LLC* [2020] USDC (DDC), the FTC's ongoing (the FTC announced an Appeal in January 2026) litigation against Meta (Facebook) which was decided in the District Court in November 2025 in *FTC v. Meta Platforms, Inc.*, No. 1:20-cv-03590 (D.D.C. Nov. 18, 2025), and the combined DOJ/FTC efforts against Apple and Amazon. While these actions often draw global attention and sometimes effect changes in platform conduct, their impact has been limited by the challenges of protracted litigation, evolving technical business models, and the absence of up-front regulatory obligations tailored to digital markets.

Recognising the limits of reactive, case-by-case enforcement, a number of states (including California) have moved to develop targeted digital regulation. The *California Consumer Privacy Act* and the *California Privacy Rights Act* create duties of registration, transparency, and compliance for businesses handling personal data above specified thresholds. These laws grant consumers enhanced rights to access, deletion, and opt-out of data sharing, while empowering a dedicated enforcement agency (the California Privacy Protection Agency) with administrative powers. Other states (including Virginia, Colorado, and Connecticut) have enacted similar statutes, creating a patchwork regulatory landscape for platforms operating nationally.

Despite numerous Congressional proposals, comprehensive federal legislation imposing registration or licensing requirements on digital platforms remains absent. The American *Innovation and Choice Online Act* and the *Open App Markets Act*, two major bills debated in Congress in 2022 to 2024, proposed to impose up-front conduct obligations and non-discrimination requirements on 'covered platforms' designated according to size and influence, but neither became law (ACCC, 2025). As a result, regulatory supervision remains fragmented, and ex ante obligations are rare.

Federal agencies have, however, pursued voluntary codes of conduct, negotiated settlements (with prescribed compliance, monitoring, and corporate structural changes), and orders requiring ongoing reporting or external audits. Sectoral oversight is also emerging. For example, the financial services sector is regulated with specific entry and compliance requirements for digital wallet providers and fintech entities. In telecommunications, licensing for carriers and broadcasters persists, even as digital platform intermediaries largely escape direct licensing.

The US experience highlights both the effectiveness and the limits of adversarial enforcement against digital platforms. Without a robust system of mandatory registration or licensing for digital platforms, regulatory action is reactive and piecemeal, with the result that platform business models continue to outpace legal adaptation. Recent federal policy shifts signal growing interest in pre-designation of powerful platforms, but as at 2025, the United States largely remains an exception among developed economies in not requiring sectoral licensing for digital services.

3.3 United Kingdom

In the United Kingdom, the regulation of digital platforms has shifted decisively toward ex ante supervisory obligations, backed by statutory codes and registration requirements. Two pieces of legislation anchor this approach: the *Online Safety Act 2023* (UK) and the *Digital Markets, Competition and Consumers Act*.

The *Online Safety Act 2023* imposes compliance duties and registration mandates on platforms that provide user-generated content and interaction, designating them according to the scale and nature of risk. Companies within scope (including search engines and social media platforms) must actively monitor, report, and address illegal and harmful content. Registration with Ofcom, the UK's independent communications regulator, is compulsory for designated services, and non-compliance with content duties or registration obligations may trigger financial penalties, service restrictions, or criminal liability for officers.

Ofcom is further empowered to issue codes of practice specifying technical and procedural obligations. Companies must conduct risk assessments, implement reporting tools, and facilitate redress for users affected by harmful content, misinformation, or algorithmic manipulation. The regulatory model is risk-based, with supervision and enforcement tailored to the scale and impact of the platform's service.

In parallel, the *Digital Markets, Competition and Consumers Act* establishes a system for designating 'Strategic Market Status' platforms, subjecting them to tailored codes of conduct to prevent anti-competitive or unfair behaviour. The Act vests the Competition and Markets Authority with the power to impose conduct requirements, order divestitures, and mandate interoperability, data sharing, and access for third-party businesses and consumers.

Enforcement is robust, with financial penalties for breaches set at up to 10 per cent of global turnover and Ofcom able to compel information, reports, and access. The regulatory regime supports sector-wide transparency and harmonisation, aligning with EU and international benchmarks without direct replication. Platforms may appeal sanctions to independent tribunals, but the broad scope of obligations and penalties signals the seriousness of regulatory engagement.

The UK system demonstrates both the feasibility and necessity of binding platform businesses to public safety, competition, and consumer protection imperatives. Registration, licensing, and code-based regulation are not mere formalities but act as central levers for effective governance. By designating critical platforms and imposing clear duties, UK law provides a blueprint for Australian reform, balancing innovation and market vitality with enforceable responsibility and user protection (ACCC, 2025). UK Online Safety Act 2023 requires no formal platform registration with Ofcom but applies automatically to services meeting jurisdictional criteria through extraterritorial enforcement. This included fines of up to £18M/10% revenue, business disruption orders, and potential criminal liability for senior managers.

3.4 European Union

The European Union has established the world's most comprehensive and ambitious regulatory regime for digital platforms, anchored by the *Digital Services Act* (DSA) and the *Digital Markets Act* (DMA). These instruments, which came into force in 2023 to 2024, mark a decisive shift from reactive enforcement to ex ante, risk-based regulation, with mandatory registration, designation, and sector-specific obligations for digital platforms operating in the EU (European Union, 2022a, 2022b).

The DSA applies to a broad range of online intermediaries, including hosting services, online marketplaces, and social networks. It introduces a tiered system of obligations, with the most stringent requirements reserved for 'Very Large Online Platforms' (VLOPs) and 'Very Large Online Search Engines' (VLOSEs), being those with more than 45 million monthly active users in the EU. All covered services must register with the European Commission, appoint a legal representative in the EU, and comply with transparency, reporting, and due diligence duties (European Union, 2022b).

Key DSA obligations include proactive monitoring and removal of illegal content, with notice-and-action mechanisms and trusted flagger systems. Platforms must provide transparency in advertising, recommender systems, and content moderation. VLOPs and VLOSEs must conduct annual risk assessments and independent audits. User redress, complaint handling, and out-of-court dispute resolution mechanisms are required. Data access for regulators and vetted researchers must be provided to enable oversight and research into systemic risks (European Union, 2022b).

Non-compliance can result in fines of up to 6 per cent of global annual turnover, temporary service suspension, and public naming of violators. The DSA also establishes a network of Digital Services Coordinators in each Member State, with the European Commission holding direct supervisory powers over the largest platforms (European Union, 2022b).

The DMA targets 'gatekeeper' platforms, being those with entrenched and durable market power in core platform services such as search, social networking, operating systems, and online intermediation. Designated gatekeepers must register, submit to ongoing monitoring, and comply with a detailed set of obligations and prohibitions. These include prohibitions on self-preferencing, tying, and leveraging data across services. Requirements for interoperability, data portability, and access for business users are imposed. Restrictions on combining personal data without user consent apply, and mandatory notification of mergers and acquisitions in digital markets is required (European Union, 2022a).

The European Commission is empowered to investigate, impose remedies, and levy fines of up to 10 per cent of global turnover (20 per cent for repeat infringements). Structural remedies, including divestiture, may be ordered for systematic non-compliance (European Union, 2022a).

The EU regime is notable for its focus on enforceable responsibility across corporate groups and associated entities. Platforms must designate a single legal entity for compliance, but the Commission may hold parent companies and affiliates jointly liable for breaches. The DSA and DMA also provide for coordinated enforcement, with national authorities, the Commission, and the European Board for Digital Services sharing information and powers (European Union, 2022a, 2022b).

Case studies since 2023 have demonstrated the regime's impact. Major platforms have been required to overhaul content moderation, advertising transparency, and business user access, while several high-profile investigations into gatekeeper conduct are ongoing (ACCC, 2025). The EU's approach sets a global benchmark for platform regulation, combining up-front registration, clear designation, and robust enforcement with a commitment to transparency, user rights, and market contestability. For Australia, the EU model offers both inspiration and practical lessons for the design of a licensing and regulatory regime for digital platforms. The EU is partially aided in its enforcement by the differential effects of tax regimes. The primary effect is that digital platforms tend to be domiciled in Ireland.

3.5 Japan

Japan has emerged as a leader in Asia for the regulation of digital platforms, combining transparency mandates, registration requirements, and competition law enforcement in a distinctive hybrid model. Japan's primary regulatory instrument for digital platforms is the Act on Improving Transparency and Fairness of Digital Platforms, which was enacted on 27 May 2020, promulgated on 3 June 2020, and entered into force on 1 February 2021 (Ministry of Economy, Trade and Industry, 2021).

Unlike traditional licensing regimes, this legislation employs a distinctive designation system rather than requiring formal licensing or advance registration from all platform operators. The Act defines digital platforms as services that create multi-sided markets connecting product or service providers with consumers using digital technology, provided via the internet, and utilising network effects whereby mutual benefits increase as participation grows (Ministry of Economy, Trade and Industry, 2020).

The Act's regulatory structure operates through two primary mechanisms. First, the Ministry of Economy, Trade and Industry designates certain large-scale platforms as 'Specified Digital Platform Providers' based on Cabinet Order criteria that establish thresholds according to business category and scale (Clifford Chance, 2021). As of

October 2025, four categories are subject to designation: online shopping malls with domestic sales exceeding 300 billion yen annually, application stores with sales exceeding 200 billion yen, media-integrated digital advertising platforms with sales exceeding 100 billion yen, and advertising intermediary platforms with sales exceeding 50 billion yen (Ministry of Economy, Trade and Industry, 2022). Second, platforms that meet these threshold criteria but are not formally designated must submit a notification to METI using the government business identification system, with failure to submit such notification attracting a fine of up to 500,000 yen (Winston & Strawn, 2020). Japan's Act on Improving Transparency and Fairness of Digital Platforms (TFTPA) regulates commercial platform-to-business relationships (transaction terms, search rankings, fees, data usage) rather than content moderation or safety issues.

Designated platforms face three core regulatory obligations under the Act. They must disclose specified information to both business users and consumers, including criteria for refusing transactions, search ranking methodologies, data acquisition and usage terms, and payment withholding conditions, with a minimum of 15 days' advance notice required for changes to terms and conditions (Winston & Strawn, 2020). They must establish fair procedures and systems, including complaint handling mechanisms, dispute resolution procedures, and appointment of domestic managers or representatives in Japan (O'Melveny & Myers, 2021). Additionally, they must submit annual reports by the end of May covering business overview, disclosure status, complaint and dispute handling statistics, and self-evaluation of compliance (Cleary Gottlieb Steen & Hamilton, 2024).

The Act's enforcement mechanisms reflect a co-regulatory philosophy that emphasises voluntary compliance while maintaining government oversight capacity. METI reviews annual reports with stakeholder input and publishes evaluations of each provider's transparency and fairness, with designated providers expected to make voluntary improvements based on these assessments (Ministry of Economy, Trade and Industry, 2024). Where platforms fail to properly disclose required information or establish adequate procedures, the METI Minister may issue public recommendations, followed by public orders if recommendations are not followed (Winston & Strawn, 2020). METI officials possess inspection powers to enter offices and examine documents, and the Minister must request Japan Fair Trade Commission action under the *Antimonopoly Act* when violations involve acts performed against large numbers of providers with significant disadvantage (Clifford Chance, 2021).

The penalty structure under the Act is relatively modest compared to other digital platform regulations. Failure to comply with METI orders regarding disclosure obligations attracts fines of up to one million yen, while failure to file annual reports, omission of required information, fraudulent statements, or failure to submit required notifications attract fines of up to 500,000 yen (O'Melveny & Myers, 2021). However, the regulatory impact extends beyond these financial penalties through reputational enforcement, as METI's public evaluations create significant reputational risks, and non-compliance can trigger referral to the JFTC for antimonopoly enforcement with potentially more substantial administrative monetary penalties (Clifford Chance, 2021). The Act applies extraterritorially to all operators providing services to the Japan market regardless of their location (O'Melveny & Myers, 2021).

Japan's regulatory approach is increasingly harmonised with global trends. The government participates in international fora on digital regulation, and recent amendments to the Act have expanded its scope to cover additional platform types and strengthen reporting and enforcement mechanisms. The Japanese experience demonstrates the value of targeted, sector-specific registration and transparency requirements, especially when combined with robust competition law oversight. For Australia, Japan's model offers a pragmatic template for incremental reform, being one that balances innovation and market access with enforceable standards of fairness, transparency, and public accountability. Japan's platform regulation law has mandatory designation requirements but reveals critical scope limitations. Although it enforces platform-to-business transparency obligations, it fails to address rampant consumer fraud on Meta platforms. The reason is that the legislation exclusively protects business users, not end consumers.

3.6 South Korea

South Korea's approach to platform regulation operates primarily through the *Telecommunications Business Act* (TBA), which establishes a comprehensive licensing and registration framework for telecommunications services that encompasses digital platforms. Under the TBA's classificatory scheme, digital platforms are categorised as Value-Added Telecommunications Services, defined as online services using core telecommunications network infrastructure, including internet-based services such as cloud computing, email, e-commerce platforms, social networking services, and online content distribution (Bae Kim & Lee, 2024). This classification subjects digital platforms to registration or reporting requirements distinct from the more stringent licensing regime applicable to core telecommunications services involving network infrastructure ownership.

The registration framework for VATS providers operates as a mandatory precondition to commencing business operations. Platforms providing value-added telecommunications services must file a report with the Ministry of Science and ICT that includes a schematic diagram of the telecommunications network to be used, detailed descriptions of user protection measures, and particulars of technical measures to prevent online copyright infringement (Bae Kim & Lee, 2024). The reporting process typically requires several days and is generally considered procedurally straightforward, though failure to comply with reporting obligations can result in corrective orders and administrative penalties (Korean Law Information Centre, 2012). Small-scale providers with capital of 100 million won or less are exempt from the reporting requirement, though this exemption ceases to apply if capital subsequently exceeds this threshold (Korean Law Information Centre, 2012).

Significant amendments to the TBA in May 2020, which took effect in December 2020, expanded regulatory obligations for large-scale VATS providers. These amendments require value-added service providers meeting certain thresholds based on user numbers and traffic volumes to take measures necessary to supply convenient and stable services to users, including maintaining network quality through traffic optimisation and load balancing (Bae Kim & Lee, 2020). For offshore VATS providers lacking a local address or business presence in Korea, the amendments mandate appointment of a local representative to handle tasks associated with protecting users' interests, including responding to user complaints and meeting regulator requests for information (Bae Kim & Lee, 2020). As a practical matter, Meta has not formally registered as a Value-Added Telecommunications Service Provider with South Korea's MSIT. However, it was designated subject to TBA requirements in 2021 and partially complies by appointing a local representative. Further amendments effective from 1 January 2024 extended these network quality maintenance requirements, with large-scale providers now required to take technical and administrative measures to ensure network quality and publish reports on the stability of their telecommunications services (Bae Kim & Lee, 2024).

The TBA's enforcement mechanisms provide Korean regulators with substantial powers to ensure platform compliance. The Korea Communications Commission and MSIT serve as the primary regulatory bodies responsible for monitoring and enforcing telecommunications regulations (Bae Kim & Lee, 2024). The KCC may issue corrective orders requiring platforms to cease violations or take specified remedial actions, and Article 53 of the TBA authorises the imposition of penalty surcharges of up to three per cent of turnover for violations, including failure to submit business reports or abide by information provision orders (Korean Law Information Centre, 2012). Where it is difficult to calculate turnover, penalties not exceeding one billion won may be imposed (Korean Law Information Centre, 2012). Additional administrative fines of up to 10 million won apply for failures to notify users of service suspensions or other specific violations (Kim & Chang, 2025).

Recent enforcement actions demonstrate the Korean regulators' willingness to apply these powers to foreign platform operators. In February 2024, the KCC imposed administrative penalties and fines of approximately 450 million won on Twitch for multiple violations including unjustified service quality restrictions and failure to implement adequate technical measures against illegal content (Chambers and Partners, 2025). In October 2023, the KCC announced provisional plans to impose penalties of 47.5 billion won on Google and 20.5 billion won on Apple for violations related to forced in-app payment practices, with proposed amendments seeking to double the maximum penalty to six per cent of relevant revenue (Chambers and Partners, 2025). The Korean regulatory approach also extends to data protection enforcement, with the Personal Information Protection Commission imposing substantial penalties on foreign entities including Meta and AliExpress in 2024 (Chambers and Partners, 2025).

Beyond the telecommunications framework, South Korea has pursued additional platform-specific regulatory initiatives. The Korea Fair Trade Commission (KFTC) released Guidelines for Review of Abuse of Dominance and Unfair Trade Practices by Online Platform Operators in January 2023, providing guidance on market definition, dominance assessment, and anticompetitive effects analysis for digital platforms (Cleary Gottlieb Steen & Hamilton, 2023). The KFTC has also conducted extensive market monitoring through surveys of online platform sectors to identify unfair trade practices and devise appropriate policy responses. While proposals for ex ante platform regulation modelled on the European Union's Digital Markets Act were abandoned by the KFTC in September 2024 in favour of amendments to existing competition law, the Ministry of Science and ICT continues to pursue a dual approach of promoting self-regulation while establishing legal frameworks for targeted regulation through further TBA amendments (Chambers and Partners, 2025).

Both Japan and South Korea demonstrate that jurisdictions can impose meaningful regulatory obligations on digital platforms without necessarily adopting formal licensing regimes equivalent to those applied to traditional regulated industries. Japan's designation and notification system establishes transparency and procedural fairness requirements for large platforms while maintaining regulatory flexibility through co-regulation principles. South Korea's telecommunications framework subjects platforms to registration or reporting requirements as a precondition to operations, with substantial penalties available for non-compliance. These approaches illustrate how regulatory frameworks can mandate platform registration or notification coupled with ongoing obligations and enforcement mechanisms, creating accountability structures that extend beyond purely voluntary industry self-regulation.

3.7 Conclusion

The comparative analysis of regulatory frameworks across the United States, United Kingdom, European Union, Japan, and South Korea reveals a decisive global shift toward ex ante regulation of digital platforms. While each jurisdiction has adopted approaches reflecting its particular legal traditions, institutional arrangements, and policy priorities, several critical commonalities emerge that hold significant implications for Australia's regulatory reform agenda.

First, mandatory registration or licensing requirements have become the norm rather than the exception among advanced economies. Whether through the EU's comprehensive DSA designation system, the UK's Ofcom registration regime, Japan's METI notification framework, or South Korea's telecommunications-based registration, leading jurisdictions have recognised that voluntary compliance and reactive enforcement are insufficient to govern platform conduct effectively. These registration mechanisms serve multiple functions. They establish regulatory visibility over market participants, create jurisdictional hooks for enforcement, enable ongoing monitoring and supervision, and provide the foundation for tailored compliance obligations.

Second, regulatory frameworks increasingly employ risk-based and proportionate approaches that differentiate obligations according to platform scale, market power, and potential for harm. The EU's tiered system distinguishing VLOPs from smaller intermediaries, the UK's graduated duties under the Online Safety Act, and Japan's threshold-based designation criteria all demonstrate sophisticated regulatory design that seeks to balance innovation incentives with public protection imperatives. This proportionality principle addresses concerns about regulatory burden while ensuring that the most significant platforms face commensurate accountability.

Third, enforcement mechanisms have evolved far beyond traditional competition law remedies to encompass substantial administrative penalties, service restrictions, and structural interventions. Financial penalties now regularly reach significant percentages of global turnover (up to 10 per cent under the EU DMA, up to 10 per cent under UK legislation, and escalating percentages under Korean law). These penalty levels reflect regulatory determination to create meaningful deterrence for non-compliance by entities whose revenues often exceed the GDP of small nations. Moreover, regulators increasingly possess powers to impose operational restrictions, mandate structural changes, and compel ongoing compliance monitoring, moving beyond one-time sanctions toward sustained regulatory engagement.

Fourth, extraterritorial application and mechanisms for reaching cross-border conduct have become standard features of platform regulation. The EU's approach of holding parent companies and affiliates jointly liable, Japan's requirement for local representatives, South Korea's local representative mandate for offshore providers, and the UK's broad territorial scope all address the fundamental challenge of governing multinational digital enterprises. These provisions recognise that effective regulation cannot be frustrated by corporate structure manipulation or jurisdictional arbitrage.

Fifth, transparency obligations regarding platform operations, algorithmic decision-making, content moderation, and business practices form a consistent thread across jurisdictions. Requirements to disclose ranking criteria, explain suspensions or restrictions, provide appeal mechanisms, and report compliance metrics reflect a shared understanding that platform power derives partly from information asymmetry and that effective governance requires rendering platform operations visible to regulators, business users, and consumers.

The international experience examined in this chapter decisively undermines arguments that digital platform regulation is either infeasible or economically harmful. The jurisdictions analysed include some of the world's most dynamic and innovative economies, yet all have concluded that market forces alone cannot adequately discipline platform conduct or protect public interests. Moreover, the proliferation of regulatory frameworks has not prevented continued platform growth or technological innovation. Rather, it has created more contestable markets, better-protected users, and more accountable corporate conduct.

For Australia, several lessons emerge with particular clarity. The absence of mandatory registration or licensing for platform businesses represents a significant gap in the regulatory architecture, leaving Australian markets and consumers exposed to risks that peer jurisdictions have moved decisively to address. The patchwork of existing consumer protection, competition, and sectoral laws (while valuable) lacks the coherence, comprehensiveness, and ex ante orientation necessary to govern platform conduct effectively in 2025 and beyond.

Australia need not reinvent regulatory approaches from first principles. The frameworks examined in this chapter provide tested models that Australia can adapt to its particular circumstances, institutional arrangements, and policy objectives. A registration and licensing regime for digital platforms operating in Australia could draw upon Japan's pragmatic designation and transparency approach, the EU's sophisticated tiering and enforcement mechanisms, the UK's risk-based supervisory model, and South Korea's telecommunications-anchored framework. Such a regime would place Australia firmly within the international mainstream of platform governance while maintaining flexibility to tailor obligations to Australian conditions.

The regulatory convergence documented in this chapter reflects not regulatory overreach but rather a mature understanding among democratic market economies that digital platforms (because of their scale, network effects, data advantages, and integration into economic and social life) require governance frameworks commensurate with their power and impact. Australia's regulatory response should reflect this same understanding, establishing registration and licensing requirements that ensure accountability, transparency, and compliance with Australian law while preserving the genuine benefits that digital platforms can provide to businesses and consumers.

3.8 References

Australian Competition and Consumer Commission. (2025). *Digital platform services inquiry: Final report (March 2025)*. Commonwealth of Australia.

Bae Kim & Lee LLC. (2020, May 20). Korea passes telecom law amendment that will require major content providers (CPs) to take measures for maintaining "stable" services, and, if offshore, to appoint local representative. *Lexology*. https://www.lexology.com/library/detail.aspx?g=c6b34562-8cc1-43d8-91bb-b5e9652c6cb7

Bae Kim & Lee LLC. (2024). In brief: Telecoms regulation in South Korea. *Lexology*. https://www.lexology.com/library/detail.aspx?g=3a5f9c7f-e340-4050-be1a-84f957b40ae8

Chambers and Partners. (2025). TMT 2025: South Korea. *Global Practice Guides*. https://practiceguides.chambers.com/practice-guides/tmt-2025/south-korea/trends-and-developments

Cleary Gottlieb Steen & Hamilton LLP. (2023). Digital markets regulation handbook: South Korea. https://content.clearygottlieb.com/antitrust/digital-markets-regulation-handbook/south-korea/index.html

Cleary Gottlieb Steen & Hamilton LLP. (2024). Digital markets regulation handbook: Japan. https://content.clearygottlieb.com/antitrust/digital-markets-regulation-handbook/japan/index.html

Clifford Chance. (2021, August). Japan's digital platform regulations. *Talking Tech Blog*. https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2021/08/japan-s-digital-platform-regulations.html

European Union. (2022a). Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). *Official Journal of the European Union*, L 265/1.

European Union. (2022b). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act). *Official Journal of the European Union*, L 277/1.

Kim & Chang. (2025, March 28). Amendment to Enforcement Decree of the TBA to enhance user notification obligations for value-added telecom service failures. https://www.kimchang.com/en/insights/detail.kc?sch_section=4&idx=31799

Korean Law Information Centre. (2012). *Telecommunications Business Act* (Act No. 11201). https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=25944&type=new&key=

Ministry of Economy, Trade and Industry. (2020). *Summary of Act on Improving Transparency and Fairness of Specified Digital Platforms*. https://www.meti.go.jp/english/policy/mono_info_service/information_economy/digital_platforms/pdf/sum_tfdpa.pdf

Ministry of Economy, Trade and Industry. (2021, April 23). Making the digital market easier to use: The Act on Improving Transparency and Fairness of Digital Platforms. https://www.meti.go.jp/english/mobile/2021/20210423001en.html

Ministry of Economy, Trade and Industry. (2022, October 3). Designation of digital platform providers subject to specific regulations under the Act on Improving the Transparency and Fairness of Digital Platforms [Press release]. https://www.meti.go.jp/english/press/2022/1003_005.html

Ministry of Economy, Trade and Industry. (2024, February 2). Evaluation on transparency and fairness of specified digital platforms compiled [Press release]. https://www.meti.go.jp/english/press/2024/0202_002.html

O'Melveny & Myers LLP. (2021, April 1). New regulation of digital platforms in Japan. https://www.omm.com/insights/alerts-publications/new-regulation-of-digital-platforms-in-japan/

Winston & Strawn LLP. (2020, December 18). Japanese legislature passes Act to regulate Big Tech platforms. *Competition Corner Blog*. **https://www.winston.com/en/blogs-and-podcasts/competition-corner/japanese-legislature-passes-act-to-regulate-big-tech-platforms**

4 Chapter 4: Licensing and Registration as Enforcement Tools: From Principle to Practice

4.1 Introduction

The practical effectiveness of platform regulation depends not merely on the substantive obligations imposed but on the mechanisms through which those obligations become legally enforceable. This is particularly the case against entities that may have minimal physical presence in Australia and whose corporate structures are designed to frustrate jurisdictional accountability.

This chapter examines five issues that determine whether platform licensing can operate as an effective regulatory tool rather than merely aspirational policy. First, it analyses the *Scams Prevention Framework Act 2025* (Cth) as a recent legislative effort to impose obligations on digital platforms. It examines both its ambitions and its enforcement limitations. Second, it explores the relationship between registration and licensing in Australian administrative law. It argues that the distinction is narrower than commonly assumed and that registration serves as the prerequisite for lawful operation rather than merely a voluntary notification mechanism. Third, it considers whether licensing obligations should be anchored to physical infrastructure presence in Australia. To do this, it uses concepts from the *Broadcasting Services Act 1992* (Cth) to create tangible points of regulatory leverage. Fourth, it examines whether enforcement innovations from telecommunications regulation, particularly the ACMA's alphanumeric SMS rules designed to combat scams, might offer transferable insights for platform accountability. Fifth, it looks at the Australia-US Free Trade Agreement (AUSFTA) to determine whether Australia has obligations that would limit the proposed approach. In doing this, the report assumes that the AUSFTA is still on foot, despite the imposition of tariffs by the US, which are inconsistent with that agreement.

These questions are not simply technical matters of regulatory design but go to the heart of Australia's capacity to assert jurisdiction over digital platforms. Especially where platform business models depend on serving Australian users while avoiding Australian legal responsibility. International experience demonstrates that registration and licensing regimes can operate effectively even against multinational corporations (Law, 2025). However, this is only true when certain structural prerequisites are satisfied. Those prerequisites include:

(a) clear designation of who must hold a licence;
(b) mechanisms for reaching associated entities within corporate groups;
(c) connections between licensing obligations and tangible infrastructure or market access that cannot be easily relocated; and
(d) graduated enforcement tools that create genuine consequences for non-compliance.

The analysis in this chapter draws on both Australian regulatory precedents and international practice to demonstrate how these elements can be integrated into a coherent licensing framework for digital platforms.

4.2 The Scams Prevention Framework Act 2025: Obligations Without Enforcement?

The *Scams Prevention Framework Act 2025* (Cth) represents a significant legislative effort to combat the growing scourge of scams affecting Australian consumers, with digital platforms identified as critical nodes in the scam ecosystem alongside banks and telecommunications providers (Australian Treasury, 2025). The Act establishes a comprehensive regime imposing obligations on designated entities to prevent, detect, disrupt, and respond to scams, with social media services explicitly intended to fall within its scope through ministerial designation. The framework includes requirements for risk assessment and mitigation systems, customer verification and authentication measures, scam detection and blocking capabilities, information sharing with other designated entities and law enforcement, complaint handling and dispute resolution procedures, and reporting to regulators on scam incidents and preventive measures. These obligations are backed by civil penalty provisions, enabling the Australian Competition and Consumer Commission to seek substantial financial sanctions for non-compliance(Australian Treasury, 2025).

Perhaps most significantly for the present analysis, the Act requires designated entities to become members of an approved external dispute resolution scheme, which in the first instance will be the Australian Financial Complaints Authority (AFCA). This requirement mirrors provisions in other sectors including banking, insurance, and superannuation, where ombudsman membership serves as both a consumer protection mechanism and a regulatory accountability tool. The AFCA scheme provides consumers with free access to independent dispute resolution, can make binding determinations on member entities up to specified financial limits, and requires members to comply with determinations or face potential expulsion from the scheme and consequent inability to lawfully operate in the sector.

However, the Scams Prevention Framework Act shares a fundamental limitation with much platform regulation. It assumes compliance by entities that may regard Australian jurisdiction as optional. The Act applies to designated entities that provide services to Australians, but its enforcement mechanisms depend on the entity being amenable to Australian legal process (Dwyer et al., 2024). Financial penalties are of limited deterrent value if the regulator cannot effectively serve proceedings, obtain judgments, or enforce those judgments against assets held outside Australia. Similarly, the requirement for AFCA membership becomes largely symbolic if an offshore platform can simply decline to join while continuing to serve Australian users through digital infrastructure located entirely outside Australian territorial jurisdiction.

This enforcement challenge is not unique to the scams framework. It pervades the *Online Safety Act 2021* (Cth), which grants the eSafety Commissioner extensive powers to require platforms to remove harmful content but struggles to compel compliance from non-cooperative offshore entities (Dwyer et al., 2024). It limits the effectiveness of the News Media Bargaining Code, which can designate platforms for mandatory negotiation with news businesses but cannot compel participation by entities with no Australian corporate presence. And it undermines consumer protection provisions in the Australian Consumer Law (Schedule 2 to the *Competition and Consumer Act 2010* (Cth)), where remedies depend on identifying an Australian entity with sufficient assets to satisfy judgments.

It is important to note that a decision by a business to leave the jurisdiction is not one that would be interfered with by a licence. Provided that the business has no outstanding legal matters, it would be free to leave. Any requirement otherwise would run this risk of being inconsistent with Australia’s treaty obligations.

The issue is fundamentally one of jurisdictional reach and corporate accountability. Digital platforms typically operate through complex multinational corporate structures in which the entity serving Australian users may be a subsidiary with minimal local assets, while revenue, intellectual property, and operational control reside with related entities in foreign jurisdictions. This structure is not accidental but deliberately engineered to achieve tax efficiency, limit legal exposure, and maintain flexibility in responding to regulatory requirements. When Australian regulators seek to take enforcement action, they confront entities that can credibly claim to be mere service providers lacking decision-making authority, while the true controlling entities remain beyond practical reach of Australian courts.

The Scams Prevention Framework Act attempts to address this through broad definitions that capture entities providing services ‘to end-users in Australia’, regardless of where the entity is located or incorporated. However, statutory assertion of jurisdiction does not by itself overcome practical enforcement limitations. A foreign entity with no Australian assets, no Australian directors, and no Australian presence can simply ignore Australian regulatory demands if it calculates that the benefits of continued market access outweigh the reputational costs of non-compliance. The regulator is then left with blunt tools:

(a) attempting to persuade foreign counterparts to take enforcement action;
(b) seeking blocking orders to prevent Australian users accessing the service (which raises technical challenges and free expression concerns); or
(c) accepting de facto regulatory failure.

This enforcement limitation illustrates the fundamental distinction between substantive statutory obligations and licensing-based accountability frameworks. The Scams Prevention Framework Act establishes what platforms must do, but it does not establish a prerequisite structure determining who may operate. An offshore platform can choose to ignore the Act’s requirements if it calculates that the expected cost of enforcement (discounted by the probability of effective action against an offshore entity) is lower than the cost of compliance. The platform continues serving Australian users, generating Australian revenue, and operating its Australian business, all while remaining non-compliant with Australian law. Regulators can declare this unlawful, issue media releases condemning the platform, and commence enforcement proceedings, but the practical reality is that the platform operates with de facto impunity. On the other hand, continuing breach of a licence condition could lead to that licence being terminated with the effect that the business would be operating illegally.

Contrast this with a licensing regime. Under licensing, the initial question is not whether the platform complies with specific obligations but whether it is authorised to operate at all. A platform that declines to obtain a licence, or that loses its licence through non-compliance, is not merely in breach of particular substantive requirements but is operating without lawful authority. This transforms enforcement from pursuing an offshore entity for specific contraventions to preventing unauthorised market access through infrastructure-level controls. Australian telecommunications carriers can be required to block traffic to unlicensed platforms. Australian payment processors can be prohibited from facilitating transactions with unlicensed platforms. Australian advertising networks can be required to refuse inventory from unlicensed platforms. These enforcement mechanisms operate through Australian-based intermediaries that are unambiguously within jurisdiction, creating market exclusion that does not depend on the offshore platform's cooperation.

The distinction is not merely semantic but represents a fundamental shift in regulatory power. Substantive obligations rely on convincing or compelling offshore entities to comply with Australian law, a task that becomes progressively more difficult as platforms' global scale grows and their dependence on any single national market diminishes. Licensing creates Australian-based gatekeepers whose own authorisation depends on ensuring they do not facilitate unlicensed operations, shifting the enforcement burden from the offshore platform to domestic intermediaries. This approach does not guarantee perfect compliance, but it creates enforcement mechanisms that function regardless of platforms' willingness to submit to Australian jurisdiction, addressing the fundamental accountability deficit that undermines substantive regulation in the absence of licensing frameworks.

This analysis is not intended to suggest that the Scams Prevention Framework Act is futile or misconceived. On the contrary, it establishes important substantive obligations and provides enforcement mechanisms that will prove effective against entities that maintain Australian corporate presence or otherwise submit to Australian jurisdiction. However, it illustrates the crucial importance of ensuring that regulatory obligations are anchored to requirements that cannot be easily evaded through corporate restructuring or jurisdictional arbitrage. This is precisely where licensing regimes offer advantages over purely substantive regulatory requirements.

4.3 Registration and Licensing in Australian Law: More Than 'Licensing Lite'

The distinction between registration and licensing is often characterised as one of degree rather than kind, with registration described as 'licensing lite' that imposes minimal barriers to entry while creating regulatory visibility (Administrative Review Council, 1999). This characterisation, while capturing an important truth about relative regulatory intensity, obscures a more fundamental similarity in the Australian administrative law context. Both registration and licensing serve as preconditions for lawful operation in regulated sectors, creating legal frameworks in which the question is not whether an entity chooses to comply but whether the entity is permitted to operate at all.

Consider the operation of registration regimes across Australian commerce and professional practice. The Australian Business Register maintains records of entities conducting enterprise in Australia, with an Australian Business Number (ABN) serving as the basic identifier for tax and regulatory purposes. While obtaining an ABN is described as ‘registration’ rather than ‘licensing’, it is functionally mandatory for any business seeking to operate legitimately in Australia. An entity without an ABN cannot issue valid tax invoices, cannot claim GST credits, cannot access many government services or contracts, and signals to counterparties that it operates outside the recognised commercial framework. The registration creates a public record, establishes accountability relationships with government authorities, and serves as the foundation for further regulatory obligations including tax compliance, superannuation contributions, and various reporting requirements.

Similarly, the Director Identification Number (DIN) scheme established under the *Corporations Act 2001* (Cth) requires individuals serving as company directors to obtain a unique identifier that persists across all directorships. This is framed as registration rather than licensing, yet it operates as a mandatory prerequisite for lawful service as a director. Directors who fail to obtain a DIN commit strict liability offences, and companies that appoint non-compliant directors face penalties. The registration creates accountability by preventing individuals from obscuring their directorship history, enables regulators to track director conduct across multiple entities, and provides the foundation for enforcement actions when directors breach statutory duties. The absence of a DIN does not merely create inconvenience but renders directorship unlawful.

In the telecommunications sector, the distinction between registration and licensing is even narrower (Australian Communications and Media Authority, 2025). The Australian Communications and Media Authority maintains registers of carriers, carriage service providers, and radiocommunications licensees. These registers are not voluntary notification systems but rather records of entities that have obtained the legal authorisation required to provide the relevant services. A carrier licence under the Telecommunications Act 1997 is described as a licence but the public register serves as the definitive record of who holds that authority. Similarly, radiocommunications licences are listed on public registers, with the register indicating who is legally entitled to use particular spectrum. The format is registration, but the function is licensing. Provision of the service is prohibited to those not on the register.

Professional regulation provides perhaps the clearest illustration that registration and licensing are functionally equivalent in determining who may lawfully practise. The Law Society of New South Wales maintains a Register of Solicitors that lists all solicitors who hold a current, valid practising certificate and are legally entitled to practise law in New South Wales. This is described as a register, not a licensing system, yet its operation is identical to licensing. A person not on the register, cannot lawfully practise. The register is not an optional directory of practitioners who have chosen to notify the regulator of their existence. It is the definitive record of who has satisfied the fitness requirements and obtained the authorisation necessary for legal practice. Practising law without being on the register constitutes the criminal offence of engaging in legal practice while not entitled to do so, attracting substantial penalties.

The pattern is consistent across sectors. Medical registration boards maintain registers of practitioners authorised to practise medicine, and practising while unregistered is a criminal offence. The National Register of Emissions Units and Australian Carbon Credit Units records entities authorised to participate in carbon trading schemes, with registration being the precondition for lawful transactions. The Australian Health Practitioner Regulation Agency maintains national registers for health professionals, with registration determining who may use protected titles and provide regulated health services. In each case, the terminology of ‘registration’ rather than ‘licensing’ reflects historical usage and regulatory convention, but the substantive function is identical. It creates a public record of who is legally authorised to engage in particular activities and making clear that operation without registration is prohibited.

This functional equivalence has important implications for platform regulation. If a registration regime is established for digital platforms, the critical question is not whether it is formally designated as ‘registration’ or ‘licensing’ but whether it operates as a mandatory prerequisite for lawful market participation. The power of licensing is not in ceremonial approval processes but in the capacity to determine who may operate and under what conditions, with enforcement mechanisms that make non-compliance genuinely costly. A registration scheme that operates on the model of ABN, DIN, or professional registers achieves these objectives:

(a) it creates a public record of entities operating in Australia;
(b) establishes accountability relationships between those entities and regulators;
(c) provides the foundation for imposing and monitoring ongoing obligations; and
(d) makes clear that operation without registration is unlawful and subject to enforcement action.

The international precedents examined in Chapter 3 demonstrate that this approach is both feasible and effective. Japan’s Act on Improving Transparency and Fairness of Digital Platforms establishes a notification system rather than a formal licensing regime, yet designated digital platform providers are legally required to submit notifications and comply with ongoing transparency and reporting obligations. South Korea requires digital platforms to register as value-added service providers under telecommunications law, with registration being the precondition for lawful service provision. The European Union’s Digital Services Act (European Parliament & Council of the European Union, 2022) establishes designation mechanisms for very large online platforms, creating public registers of designated entities subject to enhanced obligations. In each case, the legal structure may be framed as registration, notification, or designation rather than licensing, but the functional reality is that market participation depends on regulatory compliance.

The implications for Australian reform are clear. Whether the regulatory framework is formally described as registration or licensing is less important than ensuring it operates on the principle that lawful platform operation in Australia requires regulatory authorisation, that this authorisation is conditional on satisfying fitness criteria and complying with ongoing obligations, and that operating without authorisation is subject to meaningful enforcement consequences (Afina et al., 2024). The terminology can follow Australian regulatory conventions, drawing on established models in telecommunications, corporate regulation, or professional services. What matters is the substance. If you are not on the register, you cannot lawfully operate. This principle, consistently applied across regulated sectors, provides the foundation for effective platform governance.

4.4 The Enforcement Pyramid: How Licensing Enables Graduated Accountability

The fundamental advantage of licensing over purely substantive regulation lies in the enforcement toolkit it creates. General statutory obligations, whether in consumer protection, online safety, or competition law, rely primarily on retrospective enforcement through civil or criminal penalties after breaches have occurred. Regulators must detect violations, gather evidence, commence proceedings, prove breaches to the requisite standard, and obtain judgments that may prove difficult to enforce against offshore entities with minimal Australian assets. This process is time-consuming, resource-intensive, and uncertain in outcome. Even when successful, it produces one-time remedies that do not create ongoing supervisory relationships or enable proactive intervention.

Licensing transforms this enforcement dynamic by establishing a continuous regulatory relationship in which compliance is not merely required but actively supervised, and non-compliance triggers graduated consequences calibrated to breach severity (Australian Competition and Consumer Commission, 2023). The licensing model creates an enforcement pyramid with multiple intervention points (Ayres & Braithwaite, 1992). At the base are informal engagements including compliance guidance, best practice sharing, and early warning discussions when regulatory concerns emerge. These soft interventions often prove sufficient for entities that maintain genuine compliance cultures and view licensing as a social licence requiring ongoing demonstration of fitness. They also create documented evidence of regulatory engagement that supports more serious enforcement if informal methods prove ineffective.

The second tier comprises formal directions and enforceable undertakings. When breaches are identified or systemic concerns emerge, regulators can issue compliance directions requiring specified remedial action within defined timeframes. Licensees that fail to comply face escalating consequences including financial penalties and potential licence conditions variations. Alternatively, licensees may offer enforceable undertakings committing to specific conduct or remediation, creating legally binding obligations that can be enforced directly without requiring fresh proceedings. These mechanisms, common across Australian financial services and telecommunications regulation, enable targeted intervention while preserving regulatory flexibility and avoiding the delay and expense of formal litigation.

The third tier involves variation of licence conditions and public reporting of non-compliance. Regulators can impose additional or more stringent conditions on licensees whose conduct raises concerns, effectively placing them under enhanced supervision. This might include more frequent reporting, independent audits at licensee expense, or restrictions on particular activities until compliance improves. Public reporting of breaches, compliance failures, or regulatory interventions creates reputational consequences that matter to platforms whose business models depend on user trust and advertiser confidence (Australian Communications and Media Authority, 2021). The combination of regulatory action and public transparency generates incentives for compliance that purely private enforcement cannot replicate.

The fourth tier comprises financial penalties that are meaningful precisely because licensing ensures the entity is legally present and accountable. As discussed in the context of external dispute resolution schemes, penalties against offshore entities with no Australian assets are largely symbolic. However, penalties against licensed entities that have demonstrated legal accountability as a condition of licensing become genuine deterrents. The penalties can be structured as in the *Telecommunications Amendment (Enhancing Consumer Safeguards) Bill 2025*, with maximums set at the greater of a fixed amount, multiples of the benefit derived from contravention, or percentages of turnover during the breach period, ensuring sanctions scale with entity size and breach severity (Australian Competition and Consumer Commission, 2023).

The apex of the enforcement pyramid is licence suspension or revocation. This represents the ultimate regulatory sanction, which is exclusion from the Australian market. For platforms whose business models depend on network effects and user scale, loss of access to Australia’s substantial and affluent market represents existential risk that cannot be absorbed as a cost of doing business. The credible threat of licence revocation creates deterrence far exceeding any financial penalty, while the graduated nature of the pyramid means revocation is reserved for serious, persistent, or egregious breaches where lesser interventions have failed. Importantly, once licensing is established as mandatory for lawful operation, revocation becomes practically enforceable through mechanisms including service blocking by telecommunications providers, payment processing restrictions by financial institutions, and advertising network exclusions, creating market-wide consequences that compel compliance.

This enforcement architecture stands in stark contrast to general statutory obligations that lack licensing frameworks. The Online Safety Act 2021 grants the eSafety Commissioner substantial powers to require content removal and impose penalties for non-compliance, but these powers depend on platforms’ voluntary submission to Australian jurisdiction. A platform that declines to comply faces financial penalties that may be unenforceable and blocking orders that are technically complex and politically contentious. There is no intermediate tier of graduated intervention, no ongoing supervisory relationship enabling proactive compliance monitoring, and no ultimate sanction of market exclusion backed by infrastructure-level enforcement mechanisms. The Act's remedies are binary. Either the platform complies, or the regulator pursues increasingly difficult enforcement action against an entity that may be effectively beyond reach.

Similarly, the Australian Consumer Law provides comprehensive consumer protection standards and substantial penalty provisions, but enforcement depends on identifying contraventions, commencing proceedings, and obtaining judgments against entities that may have minimal Australian presence. The ACCC's enforcement record demonstrates that even successful litigation against major platforms can take years to resolve and result in penalties that, while substantial in absolute terms, represent minor fractions of global revenue and do not create ongoing compliance obligations or supervisory relationships. The absence of licensing means there is no mechanism for imposing proactive requirements, no framework for monitoring ongoing conduct, and no graduated enforcement toolkit that enables proportionate intervention before harms become severe or systemic.

The enforcement advantages of licensing are thus not theoretical but practical and proven across multiple regulated sectors. Australian financial services regulation demonstrates how licensing enables early intervention when prudential concerns emerge, preventing failures rather than merely sanctioning them retrospectively (Australian Securities and Investments Commission, 2025). Broadcasting regulation shows how licence conditions can be tailored to particular platforms' conduct and market position, creating bespoke accountability frameworks. Telecommunications regulation illustrates how ongoing reporting and compliance monitoring create visibility that enables regulators to identify emerging issues and intervene before they escalate to consumer harm. In each case, the licensing framework transforms enforcement from episodic litigation to continuous supervision, from reactive penalties to proactive compliance management, and from binary outcomes to graduated interventions calibrated to breach severity and licensee responsiveness.

The international regulatory frameworks examined in Chapter 3 demonstrate how licensing and registration systems enable this graduated enforcement approach in practice. The United Kingdom's Online Safety Act, as discussed in Chapter 3, establishes Ofcom as the regulator with powers spanning the entire enforcement pyramid from guidance and compliance monitoring through to service restriction orders and substantial financial penalties up to ten per cent of global revenue (Law, 2025; Farrand, 2024). Ofcom's enforcement approach emphasises engagement and escalation, working with platforms to achieve compliance while retaining credible sanctions for persistent non-compliance. The registration requirement creates the initial regulatory relationship that enables this ongoing engagement, transforming enforcement from adversarial litigation to supervisory dialogue backed by serious consequences when dialogue fails.

The European Union's enforcement under the Digital Markets Act (European Parliament & Council of the European Union, 2022), detailed in Chapter 3, similarly illustrates licensing's enforcement advantages. The designation of gatekeepers creates ongoing compliance obligations monitored through mandatory reporting, algorithmic transparency requirements, and regular dialogue between platforms and the European Commission. When preliminary concerns emerge regarding potential non-compliance, the Commission can open formal proceedings, issue requests for information, and conduct inspections. This graduated approach, enabled by the designation system's creation of continuous regulatory relationships, contrasts sharply with retrospective competition law enforcement that depends on proving abuse after the fact. The Commission's preliminary findings against several designated gatekeepers in 2024 and 2025 demonstrate how ex ante obligations coupled with active supervision create enforcement opportunities unavailable under general competition law.

Japan's approach under the Act on Improving Transparency and Fairness of Digital Platforms, examined in Chapter 3, provides a further example of how notification requirements enable graduated enforcement. The Ministry of Economy, Trade and Industry's publication of compliance assessment reports creates transparency regarding platforms' adherence to specified transparency and procedural fairness obligations. Platforms that receive unfavourable assessments face reputational consequences and increased regulatory scrutiny, creating incentives for improved compliance without requiring formal enforcement action. However, the Ministry retains authority to issue improvement orders and ultimately impose penalties for serious violations, ensuring the graduated approach is backed by credible sanctions. This model demonstrates that even relatively light-touch notification systems can enable effective enforcement when coupled with ongoing monitoring and public reporting.

These international examples, while differing in institutional arrangements and regulatory intensity, share the common feature that registration, notification, or designation creates the foundation for ongoing enforcement relationships. Regulators can engage platforms proactively, monitor compliance continuously, escalate interventions proportionately, and ultimately impose serious sanctions including market exclusion when necessary. This stands in stark contrast to enforcement under general law, where regulators must await clear contraventions, gather sufficient evidence for litigation, commence formal proceedings, and obtain judgments that may prove difficult to enforce. The licensing-based approach transforms enforcement from reactive litigation to proactive supervision, creating accountability frameworks that operate continuously rather than episodically and that enable regulatory intervention before harms become severe or irreversible.

4.5 Infrastructure, Control, and Licensing: Anchoring Obligations to Physical Presence

One of the fundamental challenges in regulating digital platforms is their capacity to serve Australian users while maintaining minimal or no physical presence in Australia, complicating enforcement and enabling jurisdictional arbitrage. This contrasts sharply with traditional telecommunications, broadcasting, and infrastructure services, where regulatory obligations have historically been anchored to physical assets including transmission towers, cable networks, satellite ground stations, and data centres located within Australian territory. The question arises whether platform licensing should similarly be tied to infrastructure requirements, creating regulatory leverage through control over physical assets that cannot be relocated at will and establishing clear jurisdictional hooks for enforcement action.

The *Broadcasting Services Act 1992* (Cth) provides a useful precedent for how infrastructure-based regulation can operate. The Act defines ‘control’ of a broadcasting service not merely through corporate ownership but through control of the technical facilities used to provide the service. Section 6 establishes that a person is in a position to exercise control of a commercial television or radio broadcasting licence if they are in a position to exercise control of the provision of the service, and this includes control of the apparatus used to provide the service. This concept recognises that regulatory authority over broadcasters derives partly from the physical infrastructure required to transmit signals to Australian audiences, creating leverage points that exist regardless of corporate structure or beneficial ownership arrangements.

For traditional broadcasting, this infrastructure requirement is self-evident. Transmission cannot occur without towers, studios, and technical equipment located in Australia and operated under Australian licences. The ACMA’s licensing system for radiocommunications spectrum creates exclusive rights to use particular frequencies in particular geographic areas, and broadcasters must hold these licences to transmit legally. This infrastructure requirement means that even if a broadcaster’s ultimate parent company is foreign, the actual provision of the service depends on Australian-based assets subject to Australian regulatory authority. The regulator can inspect facilities, monitor technical compliance, and ultimately seize or shut down equipment if necessary to enforce compliance, providing enforcement options unavailable for purely digital services.

Telecommunications regulation operates on similar principles. Carriers under the *Telecommunications Act 1997* (Cth) are defined as entities that own or operate network units for carrying communications traffic, and carrier licences impose obligations regarding network deployment, service quality, consumer protection, and emergency service access. While modern telecommunications increasingly involves software-defined networking and cloud-based services that blur traditional distinctions between infrastructure and services, the regulatory framework continues to distinguish between facilities-based carriers and service providers precisely because control over physical infrastructure creates different regulatory opportunities and responsibilities. Carriers must maintain points of interconnection in Australia, make their networks available for emergency services, comply with lawful interception requirements, and submit to technical inspections by the regulator.

The question for platform regulation is whether analogous infrastructure requirements could or should be imposed. The most obvious candidate is content delivery network (CDN) infrastructure. Major digital platforms maintain or contract for extensive CDN presence in Australia, using edge servers located in Australian data centres to cache content closer to users and reduce latency. These servers constitute physical infrastructure in Australia that is essential to platform service quality, particularly for video streaming and other bandwidth-intensive services. Platforms could theoretically serve Australian users without local CDN presence, routing all traffic through offshore servers, but this would significantly degrade performance and user experience. The CDN infrastructure therefore represents an investment that platforms make to compete effectively in the Australian market, creating a potential leverage point for regulatory requirements.

A licensing regime could require platforms above specified thresholds to maintain CDN infrastructure in Australia, with that infrastructure being subject to regulatory oversight analogous to telecommunications facilities. This would not mean that regulators dictate technical architecture but rather that the presence of infrastructure creates jurisdictional hooks for enforcement, enables technical monitoring where relevant for regulatory objectives, and provides assets that could be subject to Australian court orders if necessary to compel compliance. Platforms operating without Australian infrastructure presence could still be subject to licensing requirements but would face additional scrutiny regarding their capacity to comply with Australian regulatory obligations and their amenability to Australian enforcement action.

The Broadcasting Services Act's concept of control provides a framework for thinking about how infrastructure requirements could operate. Control for licensing purposes would encompass not merely formal ownership but operational control over the infrastructure used to serve Australian users. This includes the ability to determine what content is cached on Australian servers, what data is collected from Australian users and where it is stored, what algorithms govern content recommendation and distribution, and what policies apply to content moderation and user safety. A platform that contracts with third-party CDN providers might argue it lacks direct infrastructure ownership, but if it controls what content flows through that infrastructure and how the service is configured for Australian users, it exercises control for regulatory purposes.

This approach aligns with the requirement, observed in both Japan and South Korea, for platforms to designate local representatives with authority to engage with regulators and accept service of legal process. A local representative without corresponding infrastructure presence might be merely a nominal compliance gesture, easily circumvented if the platform decides to cease cooperation. However, a requirement that combines local representative designation with minimum infrastructure commitments creates more robust accountability. The infrastructure represents sunk costs and ongoing operational dependencies that cannot be abandoned without significant business disruption, while the representative provides a clear point of contact and responsibility.

The counter-argument is that mandating infrastructure presence could be characterised as protectionist barrier to trade or discriminatory treatment of foreign providers, potentially conflicting with Australia's international trade obligations. However, this concern is overstated. Many jurisdictions impose local infrastructure or local presence requirements on regulated industries without successful trade challenges, provided the requirements are genuinely related to legitimate regulatory objectives rather than disguised protectionism. In telecommunications, requirements for network facilities and points of presence are standard regulatory practice globally. In financial services, requirements for local branches or subsidiaries are common for institutions above certain thresholds. The key is ensuring that infrastructure requirements are proportionate to regulatory objectives including enabling effective supervision and monitoring, facilitating enforcement action and legal recourse for Australian users, ensuring platforms can comply with data sovereignty and lawful access obligations, and creating accountability relationships with Australian regulators and Australian law.

An alternative or complementary approach is to frame infrastructure presence not as a hard requirement but as a factor in determining licence conditions and regulatory obligations. Platforms with substantial Australian infrastructure might face streamlined compliance processes, given that their assets create natural enforcement leverage and their local presence facilitates regulatory engagement. Platforms without Australian infrastructure would still be eligible for licensing but might be required to post bonds or maintain segregated Australian-user accounts to ensure funds are available for penalties or consumer remediation, accept additional reporting and audit obligations to compensate for reduced regulatory visibility, or designate Australian-based compliance officers with genuine authority over platform operations affecting Australian users.

The alphanumeric SMS filtering regime established by the Australian Communications and Media Authority provides an interesting parallel. To combat SMS scams, the ACMA implemented rules requiring telecommunications providers to block alphanumeric sender IDs from overseas sources unless the sender is registered and verified. This creates an infrastructure-based control point, as SMS messages must pass through Australian carriers' networks to reach Australian users, the carriers can implement filtering at the network level. The obligation falls on carriers rather than on the offshore entities sending scam messages, but the effect is to deny Australian market access to unverified senders. This model might be adapted for platforms. Rather than attempting to directly regulate offshore entities, requirements could be imposed on Australian intermediaries including payment processors, advertising networks, or CDN providers to verify that platforms seeking their services hold valid Australian licences or registrations.

The infrastructure-based approach is not a complete solution to platform regulation but offers important advantages. It creates regulatory leverage over entities that might otherwise regard Australian requirements as optional, providing tangible enforcement mechanisms beyond financial penalties. It aligns platform regulation with established principles in telecommunications and broadcasting, where infrastructure presence and regulatory obligations are intertwined. It provides practical mechanisms for monitoring and supervision, enabling regulators to verify technical compliance and investigate complaints. And it establishes that serving the Australian market at scale carries responsibilities that extend beyond terms of service agreements and corporate social responsibility commitments.

Importantly, infrastructure requirements need not be universal or uniform. A tiered system could exempt small platforms or those with minimal Australian user bases, recognising that de minimis operations should not face disproportionate barriers. Thresholds could be based on Australian user numbers, Australian revenue, market capitalisation, or combinations thereof, mirroring designation criteria in the EU's Digital Services Act or the UK's Online Safety Act. The key principle is that platforms of systemic significance, whose services are embedded in Australian economic and social infrastructure, should be required to maintain corresponding presence in Australia that enables effective regulation and creates accountability relationships commensurate with their market power.

4.6 External Dispute Resolution and the Requirement to Be Legally Accountable

One of the most powerful accountability mechanisms in Australian regulation is mandatory membership in industry-specific external dispute resolution (EDR) schemes. These ombudsman services provide consumers and small businesses with free access to independent dispute resolution, can make binding determinations on member entities up to specified financial limits, and serve as both consumer protection tools and regulatory supervision mechanisms. The Telecommunications Industry Ombudsman (TIO), the Australian Financial Complaints Authority (AFCA), and various state-based ombudsmen schemes share common features. Membership is mandatory for entities operating in the regulated sector, members must comply with the scheme's processes and determinations, and failure to comply results in potential expulsion and consequent inability to lawfully operate (Stuhmcke, 2002).

The operation of these schemes reveals an important implicit requirement that has direct relevance to platform licensing. For EDR membership to be meaningful, the member entity must be capable of being sued and held legally accountable under Australian law. This requirement is not always explicitly stated in legislation but flows inexorably from the structure and function of ombudsman schemes. Under Section 132 of the *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth), carriers and eligible carriage service providers must join and comply with the TIO scheme. Members who fail to comply with scheme requirements, including failure to pay fees or failure to comply with binding determinations, face potential enforcement action. The TIO may refer non-compliant members for debt recovery, and the Australian Communications and Media Authority has statutory powers to investigate and take enforcement action against entities that fail to join the scheme or fail to comply with scheme obligations, which can result in formal warnings, directions to comply, infringement notices, or court proceedings.

For a binding TIO determination to be effective and enforceable, the member must be an entity that can be held accountable under Australian law. This means the entity must have sufficient presence in Australia that it can be served with legal process, must have assets or revenue streams subject to Australian jurisdiction that can satisfy judgments or determinations, and must be structured such that court orders or regulatory directions are practically enforceable rather than merely theoretical. An offshore entity with no Australian assets, no Australian directors, and no Australian presence could nominally become a TIO member, but if it subsequently refused to comply with a determination, the TIO's enforcement mechanisms would prove ineffective.

This practical limitation explains why some international telecommunications companies have sought exemptions from mandatory TIO membership. These entities, typically providing niche international roaming or satellite services to Australian users while maintaining no Australian corporate presence, argue that mandatory TIO membership is impractical given their offshore structure and that compliance would impose disproportionate costs relative to their Australian revenue. The ACMA has granted such exemptions in limited circumstances, effectively acknowledging that TIO membership presupposes a level of Australian legal presence that some service providers lack. For entities that do become TIO members, Australian accountability is not merely convenient but essential to the scheme's operation.

The same logic applies to AFCA, which is designated as the EDR scheme for financial services firms under the *Corporations Act 2001* (Cth) (Australian Securities and Investments Commission, 2025). AFCA can make determinations binding on members up to specified monetary limits, but these determinations are only enforceable if the member entity is subject to Australian legal process. For AFCA membership to provide meaningful consumer protection rather than illusory assurance, members must be entities that can be compelled to comply through Australian courts if necessary. This explains why foreign financial institutions seeking to provide services to Australian retail clients typically establish Australian-licensed subsidiaries rather than attempting to serve the market directly from offshore. Licensing and EDR membership presuppose legal accountability, and legal accountability requires presence amenable to Australian jurisdiction.

The *Scams Prevention Framework Act 2025* (Cth) applies this model to digital platforms by requiring designated entities to become members of an approved EDR scheme, initially AFCA. However, as discussed earlier, this requirement confronts the problem that platforms may have minimal Australian legal presence. If a platform with no Australian subsidiary, no Australian assets, and no Australian directors nominally joins AFCA to comply with the statutory requirement, what happens when it subsequently refuses to comply with an AFCA determination? AFCA could report the non-compliance to the ACCC, and the ACCC could seek penalties for breach of the statutory EDR membership requirement, but actually obtaining and enforcing a judgment against an offshore entity with no Australian assets is a practical nullity.

This analysis suggests that EDR membership requirements, to be effective, must be coupled with legal presence requirements. One approach is to require platforms seeking to operate in Australia above specified thresholds to establish Australian-incorporated subsidiaries with sufficient capitalisation to satisfy potential claims, appoint Australian-resident directors with authority over Australian operations, or maintain segregated Australian bank accounts or bonds to ensure funds are available for determinations and penalties. These requirements mirror approaches in financial services and insurance, where regulatory licensing typically requires local incorporation or at minimum local branch registration with adequate capitalisation.

An alternative, less prescriptive approach is to make licensing conditional on demonstrating legal accountability. Platforms would be required to show, as part of the licensing application and ongoing compliance, that they are amenable to Australian legal process through either Australian corporate presence, appointment of Australian-resident agents with authority to accept service and bind the entity, provision of financial security in forms accessible to Australian enforcement (such as bank guarantees from Australian banks), or contractual submissions to Australian jurisdiction coupled with undertakings to comply with Australian court orders and regulatory determinations. Platforms that cannot or will not demonstrate such accountability would be ineligible for licensing, and their continued operation would be subject to enforcement action.

The alphanumeric SMS filtering regime provides a useful parallel for how infrastructure-based enforcement can operate where direct regulation of offshore entities proves difficult. The ACMA's rules require telecommunications carriers to block alphanumeric sender IDs from offshore sources unless the sender has been verified and registered. This shifts the compliance burden from the offshore scam operators (who are effectively beyond regulatory reach) to the Australian carriers (who must comply to maintain their licences). The carriers implement technical controls at network infrastructure points, blocking unregistered offshore senders regardless of those senders' willingness to comply with Australian law.

A similar approach could apply to platform regulation. Australian payment processors could be required to verify that platforms collecting payments from Australian users hold valid Australian licences or registrations before processing transactions. Australian advertising networks could be required to verify platform compliance before accepting advertising inventory. Australian CDN providers could be required to ensure platforms using their infrastructure maintain current licences. These obligations would fall on Australian-based intermediaries that are unambiguously subject to Australian jurisdiction, creating indirect enforcement mechanisms that do not depend on offshore platforms' voluntary compliance.

The precedent for this approach exists in various regulatory contexts. Anti-money laundering rules impose obligations on financial institutions to verify customer identity and report suspicious transactions, effectively deputising banks and other intermediaries as gatekeepers for regulatory compliance. Taxation rules require withholding by payers of certain income types, placing compliance obligations on Australian entities regardless of the residence or intentions of the foreign recipient. Pharmaceutical regulation restricts wholesale supply to licensed pharmacies, using supply chain controls to enforce retail licensing requirements. In each case, enforcement leverages entities that are clearly within jurisdiction to ensure compliance by entities that might be beyond practical reach.

The policy question is whether such intermediary-based enforcement is appropriate for platform regulation. Arguments in favour include that it creates practical enforcement mechanisms without depending on offshore platforms' voluntary compliance, leverages entities that are unambiguously subject to Australian jurisdiction and cannot easily relocate, provides regulatory visibility over platforms' Australian operations through reporting by intermediaries, and aligns with precedents in financial services, telecommunications, and other regulated sectors. Arguments against include potential over-breadth if intermediaries face liability for platforms' regulatory violations, possible reduction in service availability if intermediaries decline to work with platforms facing regulatory uncertainty, and concerns about restricting market access for smaller or newer platforms that might struggle to navigate licensing requirements.

These tensions are manageable through careful regulatory design. Safe harbours could protect intermediaries that implement reasonable verification processes in good faith. Grace periods and transitional arrangements could prevent disruption to existing services while licensing frameworks are established. Exemptions for small platforms or those with minimal Australian presence could prevent disproportionate barriers to market entry. The key insight is that legal accountability is not merely a desirable feature of licensing but a practical prerequisite for enforcement and achieving accountability may require both direct obligations on platforms and indirect enforcement through Australian-based intermediaries.

4.7 Australia-US Free Trade Agreement

4.7.1 Is a licencing regime prohibited under the Australia-US Free Trade Agreement?

The Australia-US Free Trade Agreement (AUSFTA) does not prohibit new regulatory regimes. However, digital platform licensing must be objective and "not more burdensome than necessary".

A new licensing regime that applies equally to all Australian corporations, regardless of whether their parent company is domiciled in Australia or the United States, is generally **not prohibited** by the FTA. However, for such a regime to be compliant, it must satisfy specific standards regarding transparency and proportionality. The AUSFTA governs new regulations through several key legal principles:

4.7.1.1 National Treatment (Articles 10.2 and 11.3)

The core obligation of "National Treatment" requires Australia to treat US service suppliers and investors no less favorably than it treats its own. Provided that the licensing regime applies to "all businesses in a specific class" regardless of ownership, it would likely meet this test. The AUSFTA does not prevent Australia from regulating its domestic market. It only prevents Australia from creating a "tilted playing field" that disadvantages US owned companies compared to domestic ones.

4.7.1.2 Standards for Domestic Regulation (Article 10.7)

Even if a licensing regime is non-discriminatory, it must still comply with **Article 10.7** (Domestic Regulation). Under this article, Australia must "endeavour to ensure" that any licensing requirements it creates are:

- **Objective and Transparent:** Based on clear criteria, such as the competence of the business to supply the service.
- **Not More Burdensome Than Necessary:** The regulation must be proportionate to the goal it seeks to achieve (for example, ensuring the quality of a service or protecting consumers).
- **Not a Disguised Restriction:** The licensing procedure should not, in itself, act as a barrier to supplying the service.

4.7.1.3 Market Access (Article 10.4)

The licensing regime cannot be used to limit the "Market Access" of US firms by:

- Imposing a cap on the total number of service suppliers allowed in that class.
- Requiring an "economic needs test" to prove that a new business is necessary before granting a licence.

4.7.1.4 Annex II Reservations (The "Flexibility"" List)

The agreement uses a "negative list" approach, meaning all services are covered unless specifically excluded. Australia has listed several sectors in **Annex II**, where it explicitly reserved the right to "adopt or maintain any measure" (including new, more restrictive licensing) in the future. This applies particularly to **public interest areas** such as law enforcement.

4.7.2 Is a local presence requirement prohibited under the Australia-US Free Trade Agreement?

While the Australia-United States Free Trade Agreement (AUSFTA) contains provisions that limit the ability of either country to require a local presence, it explicitly allows Australia to maintain its requirement for resident directors under the *Corporations Act 2001*. The legal framework regarding this issue is governed by two primary articles within the agreement and a specific reservation in the treaty's annexes:

4.7.2.1 The "Local Presence" Rule (Article 10.5)

Article 10.5 prohibits a party from requiring a service supplier to establish a representative office or be resident in its territory as a condition for the **cross-border supply of a service**. This rule is intended to ensure that a US company can sell services into Australia from the United States without being forced to set up a physical branch or office there.

4.7.2.2 Senior Management and Boards of Directors (Article 11.10)

For companies that choose to establish an actual investment in Australia (such as an Australian subsidiary with a U.S. parent), **Article 11.10** applies. It states that:

- A party cannot require that senior management positions be filled by individuals of a particular nationality.
- However, a party may require that a majority (or less) of the board of directors be of a particular nationality or be resident in its territory, provided this does not materially impair the investor's ability to control the investment.

4.7.2.3 The Corporations Act Reservation (Annex I)

Under the “negative list” approach, all existing laws are covered by the agreement unless they are specifically exempted in the Annexes. In **Annex I (Schedule of Australia)**, the Australian government explicitly reserved the right to maintain non-conforming measures under the *Corporations Act 2001* (Cth).

Under Section 201A of the *Corporations Act*:

- Proprietary (private) companies must have at least one director who ordinarily resides in Australia.
- Public companies must have at least three directors, at least two of whom must ordinarily reside in Australia.

Because this Act is listed as a protected measure in Annex I, the resident director requirement remains fully enforceable and is not prohibited by the AUSFTA. This requirement ensures that Australian regulators, such as ASIC, have a locally resident individual who can be held accountable for the company's governance and statutory compliance.

4.8 Conclusion

The analysis in this chapter demonstrates that platform licensing can serve as an effective accountability mechanism only if several structural prerequisites are satisfied. First, licensing or registration must operate as a genuine prerequisite for lawful operation, not merely a voluntary notification system, making clear that platforms operating without authorisation are subject to enforcement action including potential market exclusion through blocking, payment processing restrictions, and liability for intermediaries that facilitate unlicensed operations. Second, licensing must be anchored to requirements that platforms cannot easily evade, whether through infrastructure presence that creates enforcement leverage, financial security that ensures judgments can be satisfied, or EDR membership that presupposes legal accountability.

Third, the distinction between registration and licensing in Australian law is narrower than commonly assumed. Both serve as mechanisms for creating public records, establishing accountability relationships, and conditioning market participation on regulatory compliance. Whether the framework is formally designated as registration or licensing matters less than ensuring it operates on the principle that authorisation is mandatory and that unauthorised operation is prohibited. The precedents in ABN, DIN, professional registers, and telecommunications licensing demonstrate that registration can be functionally equivalent to licensing when coupled with effective enforcement.

Fourth, infrastructure requirements modelled on broadcasting and telecommunications regulation offer practical advantages for platform governance. CDN presence, data storage, local representatives, and control over technical facilities create regulatory leverage that exists regardless of corporate structure. These requirements need not be universal but can be scaled to platform size and market significance, with thresholds ensuring proportionality while requiring systemically important platforms to maintain presence commensurate with their market power.

Fifth, EDR membership requirements are powerful accountability tools but presuppose legal accountability. Platforms must be capable of being sued and subject to Australian legal process for EDR determinations to be enforceable. This may require licensing to be conditional on demonstrated legal presence through Australian incorporation, Australian-resident directors, financial security, or contractual submissions to jurisdiction. The Scams Prevention Framework Act's EDR requirement illustrates both the potential and the limitations of this approach. Mandatory membership provides important consumer protection where platforms submit to jurisdiction but becomes largely symbolic for entities that regard Australian requirements as optional.

The international experience examined in Chapter 3 demonstrates that these structural elements can be assembled into coherent regulatory frameworks. The European Union's Digital Services Act designation system, the United Kingdom's Ofcom registration regime, Japan's notification requirements with local representative mandates, and South Korea's telecommunications-based registration all create accountability relationships that extend beyond voluntary platform cooperation. Australia need not innovate from first principles but can adapt tested models to Australian circumstances, drawing on existing regulatory institutions including the ACMA's licensing administration, the ACCC's enforcement expertise, and the TIO's EDR experience.

Although the AUSFTA has been cited as a possible impediment to a licensing regime, the mechanisms for Australia to remain compliant, when the US is not, are relatively trivial.

The path forward requires legislative clarity that registration or licensing for digital platforms of systemic significance is mandatory, not optional, that licensing is conditional on demonstrating legal accountability through specified mechanisms, that infrastructure presence or equivalent commitments may be required for platforms above designated thresholds, that EDR membership presupposes capacity to be sued and held accountable under Australian law, and that enforcement mechanisms extend beyond financial penalties to include service blocking, payment restrictions, and intermediary obligations where necessary to achieve compliance. These elements, integrated into a coherent statutory framework, provide the foundation for effective platform governance that aligns digital commerce with the accountability standards applied across all systemically important sectors of the Australian economy.

4.9 References

Administrative Review Council. (1999). *What decisions should be subject to merit review?* Attorney-General's Department. **https://www.ag.gov.au/legal-system/publications**.

Afina, Y., Buchser, M., Krasodomski, A., Rowe, J., Sun, N., & Wilkinson, R. (2024). *Towards a global approach to digital platform regulation: Preserving openness amid the push for internet sovereignty* (Research Paper). Chatham House. **https://www.chathamhouse.org/2024/01/towards-global-approach-digital-platform-regulation**.

Final Text of AUSFTA. (n.d.). United States Trade Representative. Retrieved January 30, 2026, from **https://ustr.gov/trade-agreements/free-trade-agreements/australian-fta/final-text**.

Final Text of AUSFTA. (n.d.). Department of Foreign Affairs and Trade. Retrieved January 30, 2026, from **https://www.dfat.gov.au/trade/agreements/in-force/ausfta/official-documents/Pages/official-documents**.

Australian Communications and Media Authority. (2021). *Broadcasting Services – Enforcement Guidelines of the ACMA 2021* (F2021L01123). Federal Register of Legislation. **https://www.legislation.gov.au/Details/F2021L01123**.

Australian Communications and Media Authority. (2025). *Carrier Licensing Guide: Carrier licences and nominated carrier declarations*. **https://www.acma.gov.au**.

Australian Competition and Consumer Commission. (2023). *Guidelines on ACCC approach to penalties in competition and consumer law matters.* **https://www.accc.gov.au/system/files/Guidelines%20on%20ACCC%20approach%20to%20penalties%20in%20competition%20and%20consumer%20law%20matters.pdf**.

Australian Securities and Investments Commission. (2025). *Applying for and varying an AFS licence* (Regulatory Guide 1). **https://download.asic.gov.au/media/os1lodqf/rg1-published-16-june-2025-20250618.pdf**.

Australian Treasury. (2025). *Scams Prevention Framework – Protecting Australians from scams*. Australian Government. **https://treasury.gov.au/publication/p2025-623966**.

Ayres, I., & Braithwaite, J. (1992). *Responsive regulation: Transcending the deregulation debate*. Oxford University Press.

Dwyer, T., Martin, F., & Gaffey, J. (2024). Online safety and social media regulation in Australia: eSafety Commissioner v X Corp. *Australian Journal of Human Rights*, *30*, 2–18. **https://doi.org/10.1080/10383441.2024.2405760**.

European Parliament & Council of the European Union. (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). *Official Journal of the European Union*, *L* 277, 1–102. **https://eur-lex.europa.eu/eli/reg/2022/2065/oj**.

Farrand, B. (2024). How do we understand online harms? The impact of conceptual divides on regulatory divergence between the Online Safety Act and Digital Services Act. *Journal of Media Law*, *16*(2), 240–262. **https://doi.org/10.1080/17577632.2024.2357463**.

Law, S. (2025). Effective enforcement of the Online Safety Act and Digital Services Act: Unpacking the compliance and enforcement regimes of the UK and EU's online safety legislation. *Journal of Media Law*, *16*(2), 263–300. **https://doi.org/10.1080/17577632.2025.2459441**.

Stuhmcke, A. (2002). The rise of the Australian Telecommunications Industry Ombudsman. *Telecommunications Policy*, *26*(1-2), 69–85. **https://doi.org/10.1016/S0308-5961(01)00054-4**.

5 Chapter 5: Licensing, Duty of Care, and Accountability

5.1 Introduction: The Regulatory Imperative for a Digital Duty of Care

The operation of digital platforms in Australia is characterised by a profound accountability deficit. For years, these global entities have benefited from a regulatory environment predicated on industry self-regulation, a model that has been comprehensively described by parliamentary inquiry as a "failed experiment" (Joint Select Committee on Social Media and Australian Society, 2024). Platforms have engaged in what can be termed "jurisdictional arbitrage", structuring their corporate affairs to frustrate legal service, avoid local accountability, and deny effective redress to Australian users harmed by their services (JSC, 2024). This has created a situation where some of the most powerful and influential corporations in modern society operate with a degree of impunity not afforded to any other sector of the Australian economy. The final report of the Joint Select Committee on Social Media and Australian Society served as a clear policy inflection point, putting "Big Tech on notice" and asserting the urgent need to establish a meaningful social licence to operate, grounded in enforceable legal duties (JSC, 2024).

In response to this accountability gap, a strong policy consensus has emerged across major Australian inquiries, coalescing around the imposition of a statutory duty of care. This is no longer a speculative or fringe proposal. Instead, it is the settled direction of Australian policy. Recommendation 2 of the Parliamentary Committee's report called for the introduction of a "single and overarching statutory duty of care onto digital platforms for the wellbeing of their Australian users" (JSC, 2024). This was decisively echoed by the statutory review of the *Online Safety Act 2021*, known as the Rickard Report, which made as its fourth recommendation that "Australia adopt a singular and overarching duty of care that encompasses due diligence, and is underpinned by safety by design principles, risk assessment, risk mitigation and measurement" (Rickard, 2025). These landmark reports establish the clear policy objective. To shift the burden of safety from individual users onto the platforms that design, control, and profit from the digital environment.

While the policy objective is clear, the critical question and the central focus of this chapter is the mechanism of implementation and enforcement. A statutory duty, however well-intentioned, remains an abstract legal principle until it is connected to a tangible regulatory framework capable of monitoring compliance and imposing meaningful sanctions for its breach. This chapter argues that a statutory licensing regime provides the most coherent, effective, and future-proofed vehicle for translating a principles-based duty of care into a tangible and enforceable system of accountability. By making a platform's very authority to operate in the Australian market contingent upon its adherence to safety obligations, a licence transforms the duty from a legal aspiration into a core, non-negotiable business imperative. This chapter will first trace the evolution of the duty of care from its common law origins to its proposed statutory form. It will then use a detailed case study to illustrate how a licensing model operationalises this duty. Following this, it will analyse established parallels in the highly regulated sectors of finance and broadcasting, where licensing already serves as a charter of public accountability. Finally, the chapter will explore the specific procedural mechanisms of a platform licence and consider its broader economic and policy implications, concluding that such a regime represents the formalisation of a new, and long overdue, social licence for the digital age.

5.2 From Common Law Principle to Statutory Obligation: Defining a Duty of Care for the Digital Environment

5.2.1 The Common Law Foundation and its Limits

The duty of care is the foundational doctrine of the modern tort of negligence, acting as the primary legal mechanism that determines when carelessness becomes actionable. Australian courts apply the distinctive "salient features approach" to establish duty of care, moving beyond the English proximity test. Seven key factors determine duty relationships (Vines, 2000):

(a) reasonable foreseeability;
(b) control and assumption of responsibility;
(c) vulnerability and reliance;
(d) knowledge;
(e) proximity;
(f) indeterminate liability concerns; and
(g) autonomy interference.

This framework provides flexibility while maintaining legal predictability through established categories.

The foundational Donoghue v Stevenson "neighbour principle" remains influential, but Australian law has evolved through legislative changes, particularly at State level that modify common law principles. These statutes require risks to be "not insignificant" and impose objective reasonable person standards while preserving judicial discretion in novel situations. The system successfully integrates traditional common law flexibility with modern regulatory precision.

Courts distinguish between negligence-based duties that develop incrementally through case law and statutory duties created by legislation with specific requirements. Professional negligence follows the modified Bolam test from Rogers v Whitaker, while workplace health and safety creates "reasonably practicable" statutory standards. Both approaches focus on preventing foreseeable harm through proportionate measures

Australian common law has undergone a significant evolution in its approach to this doctrine. Historically, liability was confined to discrete, pre-existing categories of relationships. The High Court of Australia, in a series of landmark decisions, progressively dismantled these rigid historical classifications in favour of a more unified and principled framework. The cases are:

(a) *Australian Safeway Stores Pty Ltd v Zaluzna* [1987] HCA 7
(b) *Gala v Preston* [1991] HCA 18
(c) *Hill v Van Erp* [1997] HCA 9
(d) *Perre v Apand Pty Ltd* [1999] HCA 36
(e) *Sullivan v Moody* [2001] HCA 59
(f) *Hunter and New England Local Health District v McKenna* [2014] HCA 44
(g) *Mallonland Pty Ltd v Advanta Seeds Pty Ltd* [2024] HCA 25

A pivotal moment in this transition was the decision in *Australian Safeway Stores Pty Ltd v Zaluzna* [1987] HCA 7, which abolished the complex, category-based duties of occupiers' liability and subsumed them into the general principles of negligence, asking simply whether there was a reasonably foreseeable risk of injury.

This move towards a unified theory eventually led to the development of the contemporary "salient features" approach, which represents the High Court's mature methodology for determining the existence of a duty in novel circumstances. This approach, consolidated in cases such as *Sullivan v Moody* [2001] HCA 59, moves beyond abstract tests like "proximity" and requires a multi-factorial analysis of the relationship between the parties. Crucially, it places a heavy emphasis on the concept of "coherence", assessing whether the imposition of a new duty would be consistent with existing legal principles, statutory obligations, and the overall integrity of the legal system.

While the common law provides the doctrinal foundation for a duty of care, its inherent focus on bilateral disputes renders it structurally inadequate for addressing the systemic, one-to-many nature of algorithmic harms. The common law of negligence is designed to provide corrective justice for a specific instance of harm between identifiable parties. A claim brought by an individual user against a platform for harm caused by its recommender system would likely falter on the well-established judicial reluctance to impose liability for pure economic loss where it risks exposing the defendant to an "indeterminate" class of plaintiffs. This concern, a central feature in cases like *Perre v Apand Pty Ltd* [1999] HCA 36, reflects the court's unwillingness to open the floodgates to claims from a vast and unascertainable group of people who may have suffered a similar loss. The systemic nature of platform-generated harms, which can simultaneously affect millions of users, fits squarely within this category of indeterminate liability, making a common law pathway for redress practically unviable. This doctrinal limitation necessitates a statutory solution that can address systemic risk proactively, rather than relying on reactive, individual litigation which is ill-suited to the task.

5.2.2 The Case for a Statutory, Systems-Based Duty

The limitations of the common law create a compelling case for legislative intervention. The Rickard Report provides the core rationale for this shift, arguing that a "systems approach" is the only viable method to address the sheer scale of online harm. Such an approach rightly "shifts much of the burden for remaining safe online away from individual users and onto those most capable of identifying and addressing harms – the service providers themselves" (Rickard, 2025). It moves the focus from remedying individual instances of harmful content, a task likened to a game of "whack a mole"—to mandating that platforms design their entire operational architecture with safety as a core principle (Rickard, 2025).

In designing this statutory duty, the Rickard Report explicitly considered international precedents and recommended a "singular and overarching duty of care" rather than the multiple, content-specific duties found in the United Kingdom's *Online Safety Act 2023* (Rickard, 2025). This is a critical distinction. A framework of multiple duties tied to specific types of content risks forcing the regulator and the industry back into a reactive posture, requiring systems to be assessed "after they are 'populated' with designated content, or after harm has happened" (Rickard, 2025). In contrast, a singular, overarching duty encourages a truly "upstream" and systemic approach. It compels platforms to assess the safety of their systems and design choices before harm occurs, fostering a culture of "safety by design" that is holistic rather than fragmented (Rickard, 2025).

5.3 Defining the Scope: Enduring Categories of Harm

To give substance to this overarching duty, its scope must be clearly defined. A purely abstract duty to "prevent foreseeable harm" would be too vague to be effectively enforced. The Rickard Report provides a robust solution by proposing that the duty be anchored to a set of "enduring categories of harm". Recommendation 5 of the report specifies that the harms requiring particular attention under a duty of care should, at a minimum, include (Rickard, 2025):

(a) harms to young people, including child sexual exploitation and abuse;
(b) harms to mental and physical wellbeing, such as the promotion of self-harm or disordered eating;
(c) the instruction or promotion of harmful practices;
(d) threats to national security and social cohesion, such as violent extremist content; and other illegal content, conduct, and activity.

This approach provides a principles-based yet concrete foundation for the duty. It gives platforms clear guidance on the specific risk domains they are required to assess and mitigate. Furthermore, by framing the duty around these broad, "enduring" categories, the legislation becomes technologically neutral and future-proof. It can adapt to novel harms generated by future technologies, for example, new forms of abuse in immersive or virtual reality environments, without requiring constant and reactive legislative amendment. This is a critical advantage in a sector defined by rapid and unpredictable technological change, ensuring the regulatory framework remains relevant and effective over the long term.

5.4 A Case Study: Operationalising the Duty of Care through a Platform Licence

To understand how a licensing regime transforms the enforceability of a duty of care, it is useful to move from legal theory to a practical application. This case study illustrates how a platform licence would function as the primary regulatory instrument for operationalising and enforcing the statutory duty in a real-world scenario involving algorithmic harm.

5.4.1 The Scenario: Algorithmic Amplification of Disordered Eating Content

Consider a hypothetical social media platform, “ConnectSphere”, which is popular among young Australians. Following a series of media reports and complaints from mental health organisations, the regulator (for instance, a newly empowered eSafety Commission) initiates an investigation. The investigation finds that ConnectSphere’s recommender algorithm, which is optimised to maximise user engagement, has been creating “algorithmic ‘rabbitholes’” (JSC, 2024). Users who show even a passing interest in content related to dieting or fitness are progressively fed more extreme material, including content that promotes unhealthy eating behaviours and glamorises eating disorders. This scenario directly corresponds to the “enduring category” of “harms to people’s mental and physical wellbeing” identified in the Rickard Report and reflects the evidence of algorithmic harm presented to the Parliamentary Committee (Rickard, 2025; JSC, 2024).

Under a simple statutory duty of care without a licensing framework, the regulator would face a difficult enforcement pathway. It would need to commence court proceedings and prove, to a legal standard, that ConnectSphere’s entire algorithmic system was not “reasonable” in preventing a “foreseeable” harm. This would involve complex technical evidence, arguments over industry best practice, and a lengthy and resource-intensive legal battle over a broad, principles-based obligation.

5.4.2 The Licence as the Nexus of Obligation

A statutory licensing regime fundamentally alters this dynamic. Under this model, ConnectSphere would be required to hold a “Platform Licence” as a mandatory prerequisite for lawfully offering its service to Australian users. This licence is not merely a permission to operate. Instead, it is a legal instrument that serves as the nexus of obligation, translating the abstract, overarching duty of care into a set of concrete, auditable, and enforceable conditions. The duty of care is the guiding principle of the legislation, but the licence conditions are its operational expression.

5.4.3 Licence Conditions as Codified Duties

The platform licence would contain specific, legally binding conditions that give practical effect to the duty of care. Drawing on the recommendations of the Rickard Report and the Parliamentary Committee, these conditions would include:

5.4.3.1 Mandated Risk Assessment

A condition requiring ConnectSphere to conduct, at least annually, a comprehensive risk assessment of its services. This assessment, which must be independently audited and submitted to the regulator, would be required to specifically evaluate the risk of its algorithmic systems amplifying content that falls within the legislated "enduring categories of harm", including content promoting disordered eating (Rickard, 2025). This directly implements the core risk assessment cycle proposed in Recommendation 6 of the Rickard Report.

5.4.3.2 Safety by Design and Risk Mitigation

A condition mandating that ConnectSphere implement and document the "reasonable steps" and "safety by design" principles it has taken to mitigate the risks identified in its assessment (Rickard, 2025). In this case study, such steps would not be optional best practice. They would be a mandatory licence requirement. Examples could include de-ranking or demonetising harmful content, proactively inserting authoritative health information from organisations like the Butterfly Foundation into the feeds of at-risk users, and redesigning the recommender system to incorporate "circuit breakers" that prevent users from being drawn into harmful feedback loops (JSC, 2024).

5.4.3.3 Transparency and User Control

A condition requiring ConnectSphere to provide its users with meaningful control over their recommender systems, such as the ability to reset their algorithmic profile, as called for in Recommendation 4 of the Parliamentary Committee's report (JSC, 2024). It would also mandate transparency regarding its content moderation policies and the high-level logic of its algorithms, mirroring principles in the European Union's *Digital Services Act* (JSC, 2024).

5.4.4 The Transformation of Enforceability

The introduction of these licence conditions creates a crucial shift in the enforcement paradigm. The regulator's task is no longer to prove a nebulous breach of a general duty. Instead, it can focus on clear, objective, and verifiable compliance with specific licence conditions. A failure by ConnectSphere to submit a compliant, audited risk assessment on time is not an abstract failure of care; it is a direct and unambiguous breach of a specific licence condition. Similarly, a failure to implement the mitigation measures detailed in its own risk management plan constitutes a clear breach.

This transforms the enforcement process from complex, high-stakes litigation into a more agile and effective administrative action. For a breach of a licence condition, the regulator can deploy a graduated range of enforcement tools. It could issue a formal warning, give a remedial direction ordering the platform to come into compliance by a certain date, or issue a significant infringement notice. For serious or repeated breaches, the regulator could commence court proceedings seeking a civil penalty. The ultimate sanction, and the source of the regime's power, would be the ability to seek the suspension or cancellation of the licence itself, effectively removing the platform's authority to operate in Australia.

This model makes the duty of care tangible, measurable, and administratively enforceable. The breach of a licence condition serves as a direct and enforceable proxy for a breach of the underlying duty, providing the regulator with a clear and efficient pathway for action. It creates a system of continuous monitoring and accountability, replacing the impracticality of ad hoc litigation with the certainty of ongoing regulatory supervision.

5.5 Parallels in Precedent: Licensing as a Charter of Accountability in Finance and Broadcasting

The proposal to license digital platforms is not a radical or unprecedented regulatory intervention. Rather, it represents the application of a well-established Australian regulatory tradition to a new and powerful sector. By examining the existing licensing regimes in financial services and broadcasting, it becomes clear that licensing has long been the primary tool used to impose duties of care and create direct accountability relationships for industries that have a systemic impact on the public. These sectors provide a robust blueprint for how a platform licence would function as a charter of public accountability.

5.5.1 The Financial Services Model: Codifying a Duty of 'Efficient, Honest, and Fair' Conduct

The Australian Financial Services Licence (AFSL) regime, administered by the Australian Securities and Investments Commission (ASIC), provides the most direct legislative precedent for a platform licensing model. The cornerstone of the AFSL regime is the general obligation found in section 912A(1)(a) of the *Corporations Act 2001*. This provision requires licensees to "do all things necessary to ensure that the financial services covered by the licence are provided efficiently, honestly and fairly" (ASIC, n.d.-a; ProFinancial, 2025a; Sophisticated Investor, 2025).

This "'Efficient, Honest, and Fair Obligation" functions as a comprehensive, principles-based statutory duty of care (Sophisticated Investor, 2025). It is a powerful, standalone duty that can be breached even if no other specific provision of the Act has been contravened (Sophisticated Investor, 2025). ASIC enforces this duty directly through the licensing framework. A company's ability to provide financial services is entirely contingent on its holding an AFSL and complying with its conditions. The AFSL framework provides a direct blueprint for the proposed platform licence by demonstrating how a high-level, principles-based duty is operationalised through specific, mandatory licence conditions. These conditions require licensees to have, for example, adequate risk management systems, internal and external dispute resolution procedures, and sufficient financial, technological, and human resources to provide their services competently (ASIC, n.d.-a; ProFinancial, 2025a).

The enforcement powers available to ASIC for a breach of these obligations are severe, including the ability to impose significant civil penalties, vary, suspend, or cancel the licence, and issue banning orders against individuals (Legal Analysis, 2024b). This demonstrates how a licence creates a direct and powerful accountability relationship between the licensee and the regulator, where the ultimate sanction is the removal of the right to participate in the market.

5.5.2 The Broadcasting Model: A Social Licence for Media Technologies

The broadcasting licensing regime, administered by the Australian Communications and Media Authority (ACMA), offers a different but equally relevant parallel. A broadcasting licence, issued under the *Broadcasting Services Act 1992*, functions as a form of “social licence”. It is the legal instrument that ensures a private entity, using a public resource (the broadcasting spectrum), operates in a manner consistent with the public interest objectives articulated in the Act. These objects include promoting a diverse range of services, encouraging respect for community standards, and placing a high priority on the protection of children from harmful program material (*Broadcasting Services Act 1992* (Cth)).

The licence conditions translate these broad, public interest objectives into specific, enforceable rules governing content, local news provision, and compliance with industry codes of practice (ACMA, n.d.-a; *Broadcasting Services Act 1992* (Cth)). ACMA is empowered with a range of graduated enforcement tools to ensure compliance, including the power to issue remedial directions for breaches of licence conditions or codes of practice, and ultimately, to suspend or cancel a licence for serious or repeated non-compliance (*Broadcasting Services Act 1992* (Cth); ACMA, 2021).

This comparative analysis frames the licensing of digital platforms not as a novel form of market intervention, but as the next logical step in a long Australian tradition of using licensing to manage the social impact of powerful media and communications technologies. From radio to television, and now to digital platforms, the consistent regulatory response to the emergence of a systemically influential technology has been to create a direct accountability relationship with the public through a licensing framework. It establishes that when a service becomes integral to public discourse and social connection, its right to operate becomes conditional on its adherence to clearly defined public interest obligations.

Table 1 below provides a structured comparison of these regimes, illustrating the common architectural features that make licensing an effective accountability framework.

Table 1: Comparative Analysis of Licensing Regimes as Accountability Frameworks

Feature	Broadcasting Licence (ACMA)	Financial Services Licence (ASIC)	Proposed Platform Licence (eSafety)
Legislative Basis	Broadcasting Services Act 1992	Corporations Act 2001	Proposed *Online Safety Act* amendments

Feature	Broadcasting Licence (ACMA)	Financial Services Licence (ASIC)	Proposed Platform Licence (eSafety)
Core Statutory Obligation	Objects of the Act (e.g., community standards, child protection)	"Efficiently, honestly and fairly" (s912A)	"Overarching duty of care"
Key Licence Conditions	Content rules, local content, technical standards	Risk management, dispute resolution, competence, resources	Risk assessment cycle, safety by design, transparency, data access
Primary Enforcement Tools	Remedial directions, licence suspension/cancellation	Civil penalties, licence suspension/cancellation, enforceable undertakings	Civil penalties (up to 5% global turnover), remedial directions, licence suspension/cancellation
Accountability Relationship	Licensee accountable to ACMA for upholding public interest objectives.	Licensee accountable to ASIC for protecting consumers and market integrity.	Licensee accountable to regulator (e.g., eSafety Commission) for user safety and preventing systemic harm.

5.6 Procedural Mechanisms: Embodying Statutory Duties in Licence Conditions

A platform licensing regime would translate the overarching statutory duty of care into a set of clear, enforceable, and auditable procedural obligations embedded as conditions within the licence itself. These mechanisms, drawing heavily on the detailed recommendations of the Rickard Report, would form the practical architecture of accountability.

A foundational condition of any licence for a major platform would be the requirement to establish a local legal presence or appoint a nominated agent for the purpose of legal service in Australia. This directly implements Recommendations 43 and 44 of the Rickard Report and is the essential first step in resolving the problem of "jurisdictional arbitrage" identified by the Parliamentary Committee (Rickard, 2025; JSC, 2024). This condition ensures that platforms cannot evade the jurisdiction of Australian regulators and courts, making all other enforcement actions legally and practically viable.

The core operational conditions of the licence would codify the full risk management cycle as a continuous and non-negotiable business process. This would mandate, as per Recommendation 6 of the Rickard Report, that licensees complete a comprehensive risk assessment at least annually and whenever significant changes are made to the service (Rickard, 2025). This assessment would need to be independently audited and would require the platform to identify foreseeable risks of harm across the legislated "enduring categories". Crucially, the licence would also require the platform to document and implement the mitigation measures taken in response to these risks and to measure and report on their effectiveness. This creates a closed loop of assessment, mitigation, and evaluation, making safety a dynamic and iterative process rather than a static compliance exercise.

The licence would also mandate a suite of transparency and external accountability mechanisms. A key condition would be the requirement to produce an annual transparency report, making public key data on content moderation, complaints handling, and the outcomes of risk assessments, as proposed in Recommendation 10 of the Rickard Report (Rickard, 2025). Further conditions would require mandatory participation in a data access scheme for accredited independent researchers, enabling public interest scrutiny of platform operations (Recommendation 13, Rickard, 2025), and compulsory membership in a new Digital Ombudsman scheme to provide an avenue for external dispute resolution for users (Recommendation 26, Rickard, 2025).

Finally, for the largest and highest-risk platforms, the licence could impose conditions related to internal corporate governance. Following the model proposed in Recommendation 11 of the Rickard Report, a licence condition could mandate the establishment of a well-resourced and independent compliance function, with the head of compliance reporting directly to the board's audit and risk committee and dismissible only by the board itself (Rickard, 2025). This requires a regulator with genuine authority based in Australia. This would embed accountability at the highest level of corporate governance, ensuring that responsibility for safety is integrated into the core decision-making structures of the organisation. Together, these procedural mechanisms would transform the abstract principle of a duty of care into a comprehensive and robust regulatory system.

5.7 Economic and Policy Implications of a Licensing Regime

The implementation of a statutory licensing regime for digital platforms carries significant economic and policy implications, primarily centred on enhancing deterrence, fostering a proactive compliance culture, and rebuilding public trust in digital governance. These effects flow directly from the structural power that a licensing model confers upon the regulator.

The most immediate impact of a licensing regime is a dramatic strengthening of the deterrent effect of regulation. The Rickard Report's recommendation for civil penalties of up to 5% of global annual turnover, or $50 million, is a powerful financial disincentive (Recommendation 34, Rickard, 2025). However, a licensing framework introduces a sanction that is existentially significant: the potential for licence suspension or cancellation. For a multi-billion dollar global corporation, even a substantial fine can be absorbed and treated as a cost of doing business. The threat of being excluded from the Australian market entirely, however, represents a qualitatively different level of risk that cannot be easily priced into a business model. This ultimate sanction provides the regulator with credible leverage, ensuring that its directions are taken seriously and that compliance is prioritised at the highest levels of the organisation.

Beyond simple deterrence, a licensing model is uniquely effective at fostering a proactive compliance culture. In a non-licensed environment, a platform's engagement with regulation can be reactive and adversarial, focused on legally defending its actions after a harm has occurred. In contrast, the AFSL regime demonstrates that when a company's very right to operate is contingent on its ability to continuously demonstrate that it has adequate systems for compliance and risk management, this calculation changes (ProFinancial, 2025a). Compliance ceases to be a peripheral legal function and becomes a core business imperative. The ongoing obligations to conduct risk assessments, maintain adequate resources, and report to the regulator, all as conditions of retaining the licence, incentivise the integration of "safety by design" principles into the very architecture of the service (Rickard, 2025). This shifts corporate behaviour from a reactive posture of harm remediation to a proactive culture of risk prevention.

Finally, the establishment of a visible and robust licensing framework has profound implications for public trust. Years of perceived platform inaction and regulatory failure have eroded public confidence in the governance of the digital sphere (Rickard, 2025). A licensing regime, administered by a capable and well-resourced regulator like the proposed multi-commissioner Online Safety Commission (Rickard, 2025), sends a powerful signal that digital platforms are being held to the same standards of accountability as other critical sectors of the economy. It makes the accountability relationship between platforms and the Australian public explicit and transparent. This enhanced legitimacy of the regulatory system is crucial for rebuilding public trust, not only in the platforms themselves, but in the capacity of democratic institutions to effectively govern the digital age.

5.8 Conclusion: A New Social Licence for the Digital Age

The proliferation of systemic harms emanating from digital platforms necessitates a decisive regulatory response. The emerging consensus across Australian policy and legislative reviews is clear: the imposition of a single, overarching statutory duty of care is the necessary and appropriate measure to address the profound accountability deficit that currently exists. However, the declaration of such a duty is only the first step. Without a robust and effective enforcement mechanism, it risks becoming a symbolic gesture rather than a catalyst for meaningful change.

This chapter has argued that a statutory licensing regime provides the superior framework for implementing and enforcing this duty. It makes the duty legally tangible and administratively enforceable by translating its principles into specific, auditable licence conditions. This approach is not a radical departure from Australian regulatory practice but rather a logical extension of established precedents in the finance and broadcasting sectors, where licensing has long served as the primary instrument for creating a direct accountability relationship between powerful industries and the public interest. By making a platform's authority to operate in the Australian market conditional on its adherence to safety obligations, including mandated risk assessments, safety by design principles, and radical transparency, a licensing regime fundamentally realigns corporate incentives.

The procedural mechanisms embedded within a licence create a system of continuous regulatory supervision, while the credible threat of licence suspension provides a powerful deterrent that financial penalties alone cannot match. Ultimately, the introduction of a platform licence is more than a mere regulatory tool. It is the formalisation of a new social licence for the digital age. It asserts that access to the Australian market is not a right but a privilege, one that is contingent on a demonstrated commitment to the safety and wellbeing of Australian users. By bringing the digital world into alignment with the standards of responsibility and accountability expected of all systemically important industries, a licensing framework offers a coherent and powerful pathway to restoring trust and ensuring effective governance in our increasingly digital society.

5.9 Bibliography

Australian Communications and Media Authority. (n.d.-a). *Broadcasting licences*. Retrieved from https://www.acma.gov.au/broadcasting-licences

Australian Communications and Media Authority. (2021). *Broadcasting Services – Enforcement Guidelines of the ACMA 2021*. https://www.acma.gov.au/sites/default/files/2021-05/Draft%20Broadcasting%20Services%20-%20Enforcement%20Guidelines%20of%20the%20ACMA%202021_0.docx

Australian Securities and Investments Commission. (n.d.-a). *AFS licensee obligations*. Retrieved from https://www.asic.gov.au/regulatory-resources/financial-services/financial-advice/running-a-financial-advice-business/requirements-to-hold-an-afs-licence/afs-licensee-obligations/

Joint Select Committee on Social Media and Australian Society. (2024, November). *Social media: the good, the bad, and the ugly – Final report*. Parliament of Australia.

ProFinancial. (2025a). *AFS Licensee General Obligations*. Retrieved from https://profinancial.net.au/2025/09/18/afs-licensee-general-obligations/

Rickard, D. (2025, February). *Report of the statutory review of the Online Safety Act 2021*. Department of Infrastructure, Transport, Regional Development, Communications and the Arts.

Sophisticated Investor. (2025). *A Guide to the 'Honestly and Fairly' Obligation for Australian Financial Services Licence Holders under the Corporations Act*. AFSL House. Retrieved from https://afslhouse.com.au/insights/a-guide-to-the-honestly-and-fairly-obligation-for-australian-financial-services-licence-holders-under-the-corporations-act/

Vines, P. (2000) *The Needle in the Haystack: Principle in the Duty of Care in Negligence* UNSW Law Journal 23(2) from 35.

6 Conclusions

This report has demonstrated that the absence of mandatory licensing for digital platforms operating in Australia represents both regulatory anomaly and enforcement failure. Across four substantive chapters, the analysis has established that the constitutional authority for platform licensing is robust, that universal business regulation provides clear precedent and rationale, that international practice offers tested models for adaptation, and that licensing provides the superior mechanism for operationalising emerging statutory duties of care. The case for legislative action is compelling, grounded in legal authority, policy necessity, and practical experience from both Australian sectoral regulation and international platform governance.

The constitutional foundations examined in Chapter 1 confirm that the Commonwealth possesses multiple heads of power supporting platform licensing requirements. The telecommunications power has underpinned the evolution of carrier and carriage service provider regulation under the Telecommunications Act 1997, providing natural foundations for extending obligations to digital platforms that operate communication networks or have substantial communications functions. The corporations power enables regulation of platform entities as trading or financial corporations, and critically, supports reaching associated entities and related bodies corporate that form part of global platform groups. The outcomes in Australia doctrine, developed through statute and case law, reinforces Commonwealth authority to regulate entities whose conduct has real and substantial effect within Australian jurisdiction, regardless of where those entities are incorporated or primarily operate.

Critical design elements identified include mechanisms for ensuring that licensing obligations bind not merely Australian subsidiaries but entire corporate groups exercising control over platform operations, proportionate designation criteria that distinguish platforms of genuine systemic significance from smaller services, integration with existing privacy, safety, and competition frameworks to avoid duplication and regulatory fragmentation, and graduated enforcement mechanisms appropriate to breach severity and platform scale. The Australian Competition and Consumer Commission's recommendations provide both blueprint and impetus, calling for tailored ex ante regulation, designation of principal entities with statutory liability, mandatory registration and licensing for qualifying platforms, and integration of consumer protection, competition, and safety objectives within unified frameworks.

Chapter 2's documentation of universal business regulation in Australia establishes that platform exceptionalism is inconsistent with regulatory principles governing every other systemically important sector. Corporate registration under the Corporations Act creates foundational legal identity and ongoing compliance obligations. Industry-specific licensing administered by the Australian Prudential Regulation Authority, Australian Securities and Investments Commission, Australian Energy Regulator, Australian Communications and Media Authority, and Australian Health Practitioner Regulation Agency sets entry conditions and performance standards tailored to sectoral risk. Occupational licensing upholds standards of competence and probity at individual practitioner level. These requirements are neither incidental nor optional but constitute the regulatory backbone of commercial activity, enabling identification of responsible entities, establishing transparent entry standards, facilitating regulatory supervision and consumer redress, and supporting market confidence through verification of legitimacy.

The detailed case studies spanning banking, broadcasting, telecommunications, energy, and professional services demonstrate licensing's core functions including creating public records and accountability relationships, establishing fitness criteria and ongoing performance standards, enabling graduated enforcement from warnings through remedial orders to licence revocation, and providing consumer protection through complaint mechanisms and mandatory redress schemes. Platform businesses, despite market power and societal reach exceeding many regulated industries, operate outside this comprehensive framework. This exception permits jurisdictional arbitrage, diffuses legal accountability, generates enforcement delays, and produces opaqueness in market operations. Extending licensing to platforms is not regulatory innovation but necessary evolution, bringing digital commerce within the accountability framework that has governed Australian business for generations.

The international regulatory analysis in Chapter 3 confirms that platform licensing represents global best practice rather than Australian exceptionalism. The European Union's Digital Markets Act and Digital Services Act, the United Kingdom's Online Safety Act and Digital Markets, Competition and Consumers Act, Japan's Act on Improving Transparency and Fairness of Digital Platforms, and South Korea's telecommunications-based framework all impose mandatory registration, designation criteria for systemically significant platforms, and enforceable ex ante obligations. Common features across jurisdictions include risk-based designation using quantitative thresholds and qualitative market position assessment, transparency obligations regarding algorithmic systems and content moderation practices, mandatory reporting and audit requirements enabling regulatory supervision, substantial financial penalties scaled to global revenue for non-compliance, extraterritorial application and mechanisms for reaching associated entities, and graduated enforcement including structural remedies and market exclusion.

Significantly, these frameworks have emerged in dynamic, innovative economies including the European Union, United Kingdom, Japan, and South Korea without preventing platform growth or stifling technological development. Rather, they have created more contestable markets through interoperability and data portability requirements, better-protected users through mandatory safety systems and transparent content moderation, and more accountable corporate conduct through enforceable obligations and credible regulatory supervision. The regulatory convergence reflects mature understanding that market forces alone cannot adequately discipline platform power, that legacy techniques focused on reactive enforcement are structurally inadequate, and that forward-looking, risk-based intervention is necessary to protect competition, consumers, and democratic discourse.

Australia's continued reliance on general competition law, consumer protection requirements, and sector-specific safety obligations, without platform licensing as a unifying framework, leaves markets and citizens less protected than those in peer jurisdictions. The patchwork of existing laws lacks the coherence, comprehensiveness, and ex ante orientation necessary for effective platform governance. In addition, the lack of a requirement to be legally present in the jurisdiction makes enforcement of these laws difficult if not impossible. Australia need not reinvent regulatory approaches from first principles but can adapt tested models from international experience to Australian circumstances, institutional arrangements, and policy objectives. A registration and licensing regime could draw upon Japan's pragmatic designation and transparency approach, the European Union's sophisticated tiering and enforcement mechanisms, the United Kingdom's risk-based supervisory model, and South Korea's telecommunications-anchored framework.

Chapter 4 demonstrates that platform licensing can serve as an effective accountability mechanism only if several structural prerequisites are satisfied. It showed that licensing or registration must operate as a genuine prerequisite for lawful operation. Platforms operating without authorisation are subject to enforcement action. It also argued that licensing must be anchored to requirements that platforms cannot easily evade.The chapter demonstrated that the distinction between registration and licensing in Australian law is narrower than commonly assumed. Whether the framework is formally designated as registration or licensing matters less than ensuring it operates on the principle that authorisation is mandatory and that unauthorised operation is prohibited. The chapter also suggested that infrastructure requirements modelled on broadcasting and telecommunications regulation offer practical advantages for platform governance. The key issue is to require systemically important platforms to maintain presence commensurate with their market power.

As a fundamental point, the chapter said that platforms must be capable of being sued and subject to Australian legal process for dispute resolution determinations to be enforceable.

The chapter argued that the path forward requires legislative clarity that registration or licensing for digital platforms of systemic significance is mandatory, not optional. In that context, licensing is conditional on demonstrating legal accountability through specified mechanisms. These elements, integrated into a coherent statutory framework, provide the foundation for effective platform governance that aligns digital commerce with the accountability standards applied across all systemically important sectors of the Australian economy.

Chapter 5's analysis of licensing as mechanism for duty of care demonstrates how registration requirements translate abstract legal principles into enforceable accountability frameworks. Australian policy consensus has coalesced around imposing a single, overarching statutory duty of care for user wellbeing, as recommended by the Joint Select Committee on Social Media and Australian Society and the Rickard Review. This represents fundamental shift from reactive content moderation to proactive, systems-based obligations requiring platforms to design operational architecture with safety as core principle. However, common law negligence, with its bilateral focus and reluctance to impose liability for pure economic loss affecting indeterminate classes, provides inadequate foundation for addressing systemic algorithmic harms. Statutory intervention is necessary, but a duty of care remains abstract until connected to regulatory framework capable of monitoring compliance and imposing meaningful sanctions.

Licensing provides this connection by translating duty of care principles into concrete licence conditions including safety requirements subject to regulatory monitoring, ongoing risk assessment and mitigation as fitness standards, adequate resources, systems, and governance for safety functions, transparency and reporting enabling regulatory supervision, and graduated enforcement culminating in licence suspension or revocation. Precedents in financial services and broadcasting demonstrate the efficacy of this model. Australian Financial Services Licences impose general obligations to act honestly and fairly, maintain competence and adequate resources, manage conflicts of interest, and have dispute resolution systems. Broadcasting licences similarly impose codes regarding content standards, complaints handling, and community responsibilities. Both frameworks create continuous regulatory relationships with ongoing monitoring, graduated enforcement tools, and credible deterrence through licence suspension or cancellation.

The economic and regulatory implications extend beyond compliance mechanics. Platform licensing strengthens deterrence by introducing existential risk of market exclusion that cannot be absorbed as cost of business, unlike even substantial financial penalties. It fosters proactive compliance culture by making continuous demonstration of adequate systems a condition of operation, shifting corporate behaviour from reactive harm remediation to preventive risk management. And it rebuilds public trust through transparent, robust regulatory supervision, making accountability relationships between platforms and Australian public explicit and visible. Years of perceived platform inaction and regulatory failure have eroded confidence in digital governance. A licensing regime, administered by capable, well-resourced regulators, signals that platforms are held to the same accountability standards as other critical sectors, restoring legitimacy of regulatory systems and capacity of democratic institutions to govern the digital age.

The path forward requires legislative action to establish several key elements. First, mandatory registration for all digital platforms operating in Australia or having outcomes for Australian users, creating comprehensive public register and ensuring regulatory visibility. Second, designation criteria based on quantitative thresholds including user numbers, revenue, and market capitalisation combined with qualitative assessment of market power, network effects, and systemic importance, identifying platforms subject to enhanced licensing obligations. Third, requirement for designated platforms to nominate principal entity with statutory liability for conduct of associated corporate actors, addressing jurisdictional arbitrage and creating enforceable accountability. Fourth, licence conditions incorporating statutory duties of care including systems-based safety obligations, risk assessment and mitigation requirements, transparency regarding algorithmic systems and content moderation, human review and redress mechanisms, and adequate resources and governance for compliance. Fifth, graduated enforcement mechanisms providing regulators with tools proportionate to breach severity including warnings and enforceable undertakings, compliance directions and remedial notices, civil penalties scaled to global revenue, and ultimately licence suspension or revocation with market exclusion.

Integration with existing frameworks is essential to avoid duplication and regulatory fragmentation. Platform licensing should complement privacy regulation under the Privacy Act, online safety requirements under the Online Safety Act, and competition law under the Competition and Consumer Act. Institutional arrangements should clarify regulatory roles, with Australian Communications and Media Authority potentially administering licensing, Australian Competition and Consumer Commission providing competition and consumer protection oversight, and eSafety Commissioner maintaining online safety functions. Information-sharing protocols should facilitate coordination, and potentially a Digital Platform Regulators Forum could provide ongoing interagency cooperation. International alignment should guide Australian design, with regulatory cooperation agreements facilitating enforcement against cross-border platforms and participation in multilateral forums ensuring Australian influence on evolving global standards.

The case for platform licensing rests on multiple grounds both principled and practical. It closes accountability gaps that undermine enforcement and limit consumer recourse, addressing jurisdictional arbitrage that has frustrated legal service and created diffused responsibility. It aligns digital commerce with universal business regulation standards, ending regulatory exceptionalism inconsistent with principles governing banking, telecommunications, energy, broadcasting, and professional services. It implements international best practice in platform governance, placing Australia within regulatory mainstream alongside European Union, United Kingdom, Japan, and South Korea. And it operationalises statutory duties of care through enforceable licence conditions, translating policy consensus into tangible regulatory frameworks with continuous supervision and credible deterrence.

Years of platform self-regulation have proven comprehensively inadequate. Parliamentary inquiry has described it as failed experiment. Regulatory agencies have documented persistent enforcement limitations. Statutory reviews have called for fundamental shifts toward systems-based obligations and proactive safety requirements. The time for decisive legislative action has arrived. Digital platforms are not ordinary businesses but systemically important intermediaries whose operations affect economic activity, social interaction, democratic discourse, and individual wellbeing. Their extraordinary reach and impact demand regulatory frameworks commensurate with their power, just as banking, telecommunications, and broadcasting have long been subject to licensing as recognition of their critical societal functions.

Licensing formalises a new social licence for the digital age. It asserts that access to Australian markets is not unregulated entitlement but privilege contingent upon demonstrated commitment to safety, fairness, and legal compliance. It recognises that platforms can provide genuine benefits, facilitating commerce, communication, and information access in ways that enhance productivity and connectivity, while simultaneously ensuring that these benefits are not undermined by harms, abuses, or accountability deficits. And it establishes that democratic societies retain authority to set terms of market participation, requiring enterprises whose business models depend on network effects and user data to accept responsibilities proportionate to the advantages those factors confer.

The constitutional authority for platform licensing is robust, grounded in multiple heads of Commonwealth power and supported by established telecommunications regulation. The precedent of universal business regulation is clear, demonstrated across every systemically important sector of Australian economy. International experience confirms feasibility and efficacy, with tested frameworks operational in peer jurisdictions without stifling innovation or preventing platform growth. And the mechanisms for operationalising licensing are well understood, drawing on decades of experience in financial services, broadcasting, and other regulated industries.

What remains is legislative will to act. Parliament possesses authority to establish mandatory registration, designation criteria, licence conditions, and enforcement mechanisms for digital platforms. Government possesses institutional capacity through existing regulators to administer licensing frameworks and supervise compliance. And Australian society possesses legitimate expectation that businesses operating in Australia, particularly those of systemic importance, will be subject to regulatory frameworks ensuring accountability, protecting consumers, fostering fair competition, and maintaining digital sovereignty.

The introduction of platform licensing would not merely close regulatory gap or address enforcement limitation. It would represent fundamental realignment of power and responsibility in digital economy, establishing that platforms' authority to operate is contingent rather than inherent, that market access carries corresponding obligations, and that Australian law applies with full force to all businesses serving Australian users regardless of corporate structure or jurisdictional location. By bringing digital platforms within the same framework of responsibility and accountability expected of every systemically important industry, licensing offers coherent and powerful pathway to effective governance in increasingly digital society, protecting consumers, fostering innovation within appropriate bounds, and ensuring that technological change serves rather than subverts democratic values and legal principles that have sustained Australian prosperity and social cohesion for generations.

The time for platform licensing has arrived. The constitutional foundations are established. The regulatory precedents are clear. The international models are tested. The policy consensus is formed. What is required now is legislative action to translate principle into practice, ensuring that digital platforms operating in Australia accept the same fundamental responsibility for their conduct that Australian law has always demanded of businesses wielding economic power and social influence. In so doing, Parliament would affirm that Australia's digital future will be governed by law, accountability, and democratic oversight, not by the preferences and priorities of corporations whose global reach should not exempt them from local responsibility. This is not merely regulatory reform but assertion of sovereignty, protection of citizens, and commitment to ensuring that technological transformation occurs within frameworks of law, justice, and human dignity that have long distinguished democratic societies from those where power remains unchecked and accountability remains elusive.

7 Contact

Rob Nicholls

Centre for AI, Trust, and Governance

Room L6.04 A14 The Quadrangle
The University of Sydney
NSW 2006

Phone: +61 4 1264 6477

robert.nicholls@sydney.edu.au

ellissa.nolan@sydney.edu.au

sydney.edu.au

https://www.sydney.edu.au/arts/our-research/centres-institutes-and-groups/centre-for-ai-trust-and-governance.html

CRICOS 00026A

THE UNIVERSITY OF SYDNEY

THE UNIVERSITY OF SYDNEY

Supplementary Report

Registration as an alternative to licensing

Centre for AI, Trust, and Governance

28 March 2026

Table of Contents

1 Registration as an alternative

1.1 Introduction

This supplementary report adds to the University of Sydney Centre for AI, Trust, and Governance report of 4 February 2026. That report (Report) had the title "Australia's Right to Regulate Technology: A proposal for reform". The Report proposed licensing of platforms as a key mechanism.

Feedback on the Report has suggested that the appetite for a licence regime would be greater if there was a simpler first step. It would be essential that this step could achieve the same outcomes as a licensing regime. These are:

(a) an entity in Australia that can sue or be sued;
(b) a link between that entity and products and services provided in Australia; and
(c) an assurance that the entity has the financial capacity to pay for the consequences of any legal or regulatory action taken against it.

This supplementary report outlines an approach to registration as an alternative to licensing.

1.2 Approach

This supplementary report proposes the introduction of a **Social Media Services Register** (the Register). This would require that providers of social media services that are accessible to Australian end-users to register with the Australian Communications and Media Authority (ACMA). The proposal draws its structural architecture from the Associated Newspaper Register set out in section 59 of the *Broadcasting Services Act 1992* (Cth). It employs the definitions of *social media service* and *age-restricted social media platform* taken from the *Online Safety Act 2021* (Cth).

In order to meet the requirements set out above, registration would impose three substantive obligations on each registrant:

(a) disclosure of every service the provider operates in Australia;
(b) nomination of an Australian entity with a domestic address for service, capable of suing and being sued in Australian courts on behalf of the platform; and
(c) production of a Financial Sufficiency Certificate (FSC) from a registered company auditor confirming the Australian entity holds sufficient resources to meet damages awards and pecuniary penalties. The auditor would accept direct financial responsibility for that certification, including stepping into the shoes of the platform to the extent certified if funds prove insufficient.

The scheme is modelled closely on existing Australian legislative frameworks. In particular, the foreign company local agent regime in the *Corporations Act 2001* (Cth) and the appointed actuary liability framework under the *Insurance Act 1973* (Cth). It avoids requiring the creation of a new regulatory body.

2 Policy Rationale

Social media platforms that operate in Australia but are incorporated offshore routinely present enforcement difficulties. This is the reason that the Report proposed a licensing regime. We have seen the eSafety Commission, in respect of X, face the practical impossibility of process serving. Litigants with damage in Australia have no local entity to sue. The proposed Register addresses this gap by:

(a) creating a public record of every social media service accessible in Australia and the entity responsible for it;

(b) ensuring an Australian legal entity stands behind each service and can be brought to account in Australian courts without the need for foreign service or complex jurisdictional arguments; and

(c) requiring financial substance behind that entity, certified by a professional who themselves accepts liability if the certification proves incorrect.

The proposal is intentionally narrow in scope. It does not seek to regulate the content of social media services or to impose new substantive obligations on platforms beyond those already found in the *Online Safety Act 2021* (Cth) and other Commonwealth statutes. It creates infrastructure consisting of a register and a chain of financial responsibility. It does not try to create new content regime.

3 Legislative Architecture

3.1 Structural model: section 59 of the *Broadcasting Services Act*

The proposed Register is modelled on the *Associated Newspaper Register* maintained by ACMA under section 59 of the *Broadcasting Services Act 1992* (Cth). That section requires ACMA to maintain a register of newspapers associated with the licence areas of commercial television and radio broadcasting licences. Key structural features of section 59 that are replicated in the proposal include:

(a) ACMA as the maintaining authority, with the Register accessible on the internet;

(b) a duty to enter and remove names from the Register upon satisfaction of defined conditions;

(c) the power to supply certified copies of or extracts from the Register, which are admissible in evidence in all courts and proceedings without further proof; and

(d) maintenance of the Register by electronic means.

The proposal adapts this structure by substituting the newspaper circulation thresholds with an Australian end-user nexus test. That is, a social media service must register if it is accessible to or delivered to one or more end-users in Australia. It adds a registration application process with mandatory disclosure requirements.

3.2 Definitions: *Online Safety Act*

The proposal adopts the existing statutory definitions in the *Online Safety Act 2021* (Cth) to avoid definitional inconsistency across the Commonwealth online regulatory framework. The key definitions are set out below.

3.2.1 Key Definitions from the *Online Safety Act*

Social media service (*Online Safety Act 2021* (Cth) section 13) which can be summarised as an electronic service:

(a) the sole or primary purpose of which is to enable online social interaction between 2 or more end-users;
(b) which allows end-users to link to or interact with some or all other end-users; and
(c) which allows end-users to post material.

It does not include an exempt service (none of the material on which is accessible to, or delivered to, one or more end-users in Australia).

Age-restricted social media platform (s 63C)

A broader definition inserted by the *Online Safety Amendment (Social Media Minimum Age) Act 2024* (Cth). This can be summarised as an electronic service a sole or significant purpose of which is to enable online social interaction, with the same interaction and posting conditions. This captures platforms that may not qualify as a "social media service" under section 13 of the *Online Safety Act 2021* (Cth). For example, services that are not solely or primarily social.

Provider

The entity that operates the relevant service (consistent with usage throughout the *Online Safety Act 2021* (Cth), including in Part 4A). The proposal uses "provider" to align with section 5 of *Online Safety Act 2021* (Cth).

The registration obligation proposed in this supplementary report applies to providers of both *social media services* (s 13) and *age-restricted social media platforms* (s 63C). Capturing both definitions ensures comprehensive coverage without the need to cross definitional boundaries in a new instrument.

3.3 Australian entity and address for service

The requirement that each registrant nominate an Australian entity capable of suing and being sued is closely modelled on the *local agent* framework for registered foreign companies under the *Corporations Act 2001* (Cth), Part 5B.2.[1] Under that

[1] *Corporations Act 2001* (Cth), ss 601CF–601CJ.

scheme, ASIC may not register a foreign company unless it has appointed at least one local agent who is resident in Australia. The local agent is answerable for all things the foreign company is required to do under the Act, and may be held personally liable by a court for penalties imposed on the foreign company.

Section 601CJ of the *Corporations Act 2001* (Cth) provides that a local agent is *personally liable* to a penalty imposed on the foreign company if the court is satisfied the local agent should be so liable.[2] The proposed scheme extends this logic to civil liability for damages, not merely regulatory penalties, and couples it with the Financial Sufficiency Certificate requirement described below.

3.4 Financial Sufficiency Certificate and auditor liability

The requirement for a Financial Sufficiency Certificate (FSC) from an Australian registered company auditor is the most innovative feature of the proposal. The novelty is the auditor's direct financial responsibility for that certificate. While novel in this precise configuration, it draws on several existing threads of Australian law:

3.4.1 Appointed Actuary framework (Insurance Act 1973 and Life Insurance Act 1995)

Under the *Insurance Act 1973* (Cth) and the *Life Insurance Act 1995* (Cth), general insurers and life companies must appoint an actuary who certifies the financial soundness of the entity.[3] APRA's Prudential Standard CPS 320 imposes obligations directly and personally on the Appointed Actuary. The personal responsibility for complying with those obligations continues to rest with the actuary even where the insurer has not complied. The proposed FSC regime adopts an analogous structure. The auditor accepts statutory responsibility for the accuracy of their certification. It goes further by attaching direct financial liability to that responsibility.

3.4.2 Environmental financial assurance (State and Territory frameworks)

Environmental legislation across Australia requires operators of licensed premises to provide financial assurance (typically a bank guarantee or bond) sufficient to cover the costs of remediation if the operator fails.[4] The leading example is the *Protection of the Environment Operations Act 1997* (NSW). The surety providing the bond takes on direct financial liability to the regulator up to the face value of the instrument. The proposed auditor liability mechanism is the functional equivalent. The auditor's FSC is an assurance instrument, and the auditor stands behind that instrument with their own resources. This is analogous to the surety on an environmental bond

---

[2] *Corporations Act 2001* (Cth), s 601CJ.

[3] *Insurance Act 1973* (Cth), s 39; *Life Insurance Act 1995* (Cth), s 93; APRA, Prudential Standard CPS 320 Actuarial and Related Matters.

[4] See, for example, *Protection of the Environment Operations Act 1997* (NSW), ss 295A–295E (financial assurance framework). Environmental financial assurance bonds have long required third-party sureties to guarantee the performance of regulated entities.

3.4.3 Foreign company local agent personal liability

The *Corporations Act 2001* (Cth) already contemplates that a local agent may be personally liable for obligations of a foreign corporate entity. The proposed auditor liability provision replicates this structure in a financial context: just as a local agent answers for the foreign company's regulatory obligations, the auditor answers for the financial adequacy of the Australian entity up to the amount certified.

3.5 Unsuitability of a Parent Company Guarantee

A parent company guarantee is unsuitable for four reinforcing reasons.

First, and most fundamentally, the parent controls the subsidiary. It can strip the child entity of assets, cause it to cease trading, or wind it up entirely. These are all lawful corporate decisions that leave the guarantee attached to a shell. The parent has no incentive to preserve the entity whose liabilities it has just guaranteed.

Second, the parent is almost invariably also a foreign corporation. Enforcing a guarantee against an entity incorporated in Delaware, the Cayman Islands, or Singapore requires the same cross-border enforcement machinery that the registration scheme is designed to avoid. One offshore entity guaranteeing another solves nothing.

Third, a guarantee is only as strong as the guarantor's willingness to honour it. Unlike the auditor mechanism proposed in this supplementary report, there is no independent professional standing behind the instrument with their own licence, reputation, and statutory obligations at risk. A parent can simply decline to pay and force the claimant into protracted litigation in a foreign jurisdiction.

Fourth, corporate groups restructure constantly. The parent that gives the guarantee today may have divested the relevant business, merged with another entity, or itself become insolvent by the time a claim is made. The auditor mechanism, by contrast, requires a fresh professional certificate at regular intervals, ensuring the assurance remains current and independently verified.

4 Draft Legislative Text

The following is proposed as a new Division to be inserted into the Online Safety Act 2021 (Cth), or alternatively as a standalone Part within an amendment to the Broadcasting Services Act 1992 (Cth). Either host Act would be appropriate; the Online Safety Act is preferred given it already contains the relevant definitions and the ACMA has an existing regulatory relationship with social media providers.

Division [X] — Social Media Services Register

[X]A ACMA to maintain Social Media Services Register

(1) The ACMA is to maintain a register to be known as the Social Media Services Register (the Register).

(2) The Register must, in relation to each registered provider, contain:

(a) the legal name of the provider and each trading name under which any of the provider's social media services are made available to end-users in Australia;

(b) a description of each social media service operated by the provider that is accessible to, or delivered to, end-users in Australia;

(c) the name and Australian address for service of the nominated Australian entity for the provider; and

(d) details of the Financial Sufficiency Certificate in force for the provider, including the name of the certifying auditor and the amount certified.

(3) The Register may be maintained by electronic means.

(4) The Register is to be made available for inspection on the internet free of charge.

(5) The ACMA may supply copies of or extracts from the Register certified by an authorised ACMA officer, and a copy or extract so certified is admissible in evidence in all courts and proceedings without further proof or production of the original.

[X]B Registration obligation

(1) A provider of a social media service or age-restricted social media platform that is accessible to, or delivered to, one or more end-users in Australia must apply to the ACMA for registration in accordance with section [X]C within [90] days of the commencement of this Division (for existing providers) or within [30] days of first making the service accessible to end-users in Australia (for new providers).

(2) A provider that contravenes subsection (1) is liable to a civil penalty of 500 penalty units per day that the contravention continues.

Note: *The civil penalty is consistent with penalty levels applicable to providers under Part 4A of this Act.*

[X]C Application for registration

(1) An application for registration must:

(a) be made in the form approved by the ACMA;

(b) set out the information referred to in paragraphs [X]A(2)(a) and (b);

(c) nominate an Australian entity in accordance with section [X]D; and

(d) be accompanied by a Financial Sufficiency Certificate that complies with section [X]F.

(2) The ACMA must register the provider if satisfied that:

(a) the application complies with subsection (1); and

(b) the Financial Sufficiency Certificate is in force and complies with section [X]F.

(3) The ACMA must refuse to register the provider if not so satisfied and must give the provider written notice of the refusal and the reasons for it.

[X]D Nominated Australian entity

(1) A provider must at all times maintain a nominated Australian entity in relation to each registered social media service.

(2) The nominated Australian entity must:

(a) be a body corporate incorporated in Australia, or a natural person ordinarily resident in Australia;

(b) have a registered address in Australia at which documents may be served;

(c) be capable of suing and being sued in that capacity in any court in Australia in relation to the social media services of the provider; and

(d) have given written consent to act as nominated Australian entity for the provider.

(3) The nominated Australian entity is answerable for doing all acts, matters and things that the provider is required to do under this Division.

(4) If a court makes an order for the payment of damages or a pecuniary penalty against a provider in relation to a social media service operated in Australia, and the court is satisfied that:

(a) the nominated Australian entity should be liable for the whole or part of that amount; and

(b) it is just and equitable in the circumstances for the nominated Australian entity to be so liable;

the nominated Australian entity is liable to pay that amount or that part of that amount.

Note: *This subsection is modelled on the personal liability of local agents for foreign companies under section 601CJ of the Corporations Act 2001.*

(5) A provider must notify the ACMA in writing within [7] days if the nominated Australian entity changes. The ACMA must update the Register accordingly.

[X]E Consequences of absence of nominated Australian entity

(1) If a provider does not have a nominated Australian entity, any process, notice or other document required or authorised to be served on the provider may be served on the ACMA, and service on the ACMA is taken to be service on the provider.

(2) A provider that does not have a nominated Australian entity is liable to a civil penalty of 300 penalty units per day that the contravention continues.

[X]F Financial Sufficiency Certificate

(1) A Financial Sufficiency Certificate is a certificate that:

(a) is issued by a person who is a registered company auditor within the meaning of the Corporations Act 2001 and who holds a current registration under Division 2 of Part 9.2 of that Act (the certifying auditor);5

(b) is addressed to the ACMA;

[5] Corporations Act 2001 (Cth), s 9 (definition of 'registered company auditor'). Only a registered company auditor within the meaning of the Corporations Act may issue a Financial Sufficiency Certificate under the proposed scheme.

(c) certifies that, at the date of the certificate, the nominated Australian entity holds, or has access to, financial resources sufficient to meet:

(i) any award of damages in any court in Australia against the provider in relation to any social media service operated in Australia; and

(ii) any pecuniary penalty imposed under any Commonwealth, State or Territory law against the provider in relation to any such service;

(iii) up to the amount specified in the certificate (the certified amount);

(d) specifies a certified amount of not less than [the amount prescribed by the legislative rules]; and

(e) is dated and signed by the certifying auditor.

(2) A Financial Sufficiency Certificate must be renewed at least once in each 12-month period.

(3) A provider must notify the ACMA within 7 days if a Financial Sufficiency Certificate lapses or is withdrawn. The ACMA may suspend the provider's registration pending provision of a replacement certificate.

[X]G Liability of certifying auditor

(1) A certifying auditor who issues a Financial Sufficiency Certificate takes personal financial responsibility for that certificate.

(2) If, at any time after a Financial Sufficiency Certificate is issued:

(a) a judgment for damages or a pecuniary penalty order is made against the provider in relation to a social media service operated in Australia; and

(b) the nominated Australian entity does not have sufficient financial resources to satisfy that judgment or order up to the certified amount;

the certifying auditor is liable to satisfy the shortfall up to the certified amount as if the certifying auditor were the provider.

(3) For the purposes of subsection (2), the certifying auditor is taken to stand in the shoes of the provider to the extent of the certified amount. Any person entitled to enforce the judgment or order against the provider may enforce it against the certifying auditor to that extent.

(4) The certifying auditor's liability under this section does not limit any other liability the certifying auditor may have, whether at law or in equity, in respect of the Financial Sufficiency Certificate.

(5) A certifying auditor must not issue a Financial Sufficiency Certificate unless the certifying auditor holds professional indemnity insurance in respect of this section in the amount of not less than [the prescribed amount] with an insurer approved by APRA.

Note: *This section establishes a novel but principled liability mechanism analogous to the personal obligations imposed on Appointed Actuaries under the Insurance Act 1973 (Cth) and Life Insurance Act 1995 (Cth), and the surety liability that arises under environmental financial assurance instruments. It ensures that the certification has substantive force and is not merely a paper exercise.*

[X]H Removal from Register

(1) The ACMA must remove a provider from the Register if:

(a) the provider requests removal and the ACMA is satisfied that the provider no longer operates any social media service accessible to, or delivered to, end-users in Australia; or

(b) the ACMA is satisfied that the provider has ceased to operate in Australia and has no nominated Australian entity.

(2) Removal from the Register does not affect any liability that arose while the provider was registered.

[X]I Updating the Register

(1) A registered provider must notify the ACMA in writing within [30] days of any change to the information described in paragraphs [X]A(2)(a) or (b).

(2) A registered provider that contravenes subsection (1) is liable to a civil penalty of [50] penalty units per day that the contravention continues.

(3) The ACMA may, on its own initiative, update the Register to correct errors or omissions.

[X]J Legislative rules

(1) The Minister may, by legislative instrument, make rules prescribing:

(a) the minimum certified amount for a Financial Sufficiency Certificate;

(b) the minimum amount of professional indemnity insurance to be held by a certifying auditor; and

(c) any other matters necessary or convenient to give effect to this Division.

[X]K Definitions

In this Division:

age-restricted social media platform has the same meaning as in section 63C of the Online Services Act 2021.

Australian entity has the same meaning as in section [X]D(2).

certifying auditor has the meaning given in paragraph [X]F(1)(a).

Financial Sufficiency Certificate has the meaning given in section [X]F.

nominated Australian entity has the meaning given in section [X]D.

provider has the meaning given to it in section 5 of the Online Services Act 2021.

social media service has the meaning given to it in section 13 of the Online Services Act 2021 and includes an age-restricted social media platform as defined in section 63C of the Online Services Act 2021.

5 Key Design Choices and Policy Considerations

5.1 Dual definition coverage

Requiring registration of both social media services (s 13) and age-restricted social media platforms (s 63C) ensures that platforms which fall outside the narrower s 13 definition (because, for example, social interaction is a significant but not the primary purpose of the service) remain within scope. This approach avoids platforms engineering themselves out of coverage through definitional arguments.

5.2 Civil penalty for non-registration

The proposal relies on civil penalties rather than criminal offences, consistent with the approach taken throughout Part 4A of the *Online Safety Act 2021* (Cth). A per-day penalty structure creates a continuing incentive to comply and allows the regulator to seek urgent interlocutory relief in the Federal Court.

5.3 Auditor liability: rationale and proportionality

The auditor liability provision in section [X]G is the most significant departure from existing Australian law. Its rationale is that a certification that carries no personal consequence for the certifier is a weak guarantee. The Appointed Actuary model in insurance law demonstrates that personal statutory liability can co-exist with professional practice; the proposed extension to auditors issuing FSCs follows the same logic.

Proportionality is maintained in two ways. First, the auditor's liability is capped at the certified amount. They are not exposed to unlimited liability. Second, the mandatory professional indemnity insurance requirement in section [X]G(5) ensures the auditor has access to resources sufficient to meet that liability. It also maintains market discipline (an insurer will conduct their own due diligence before underwriting).

5.4 Interaction with the Corporations Act foreign company regime

Providers that are already registered as foreign companies under the *Corporations Act 2001* (Cth) and have appointed a local agent will not automatically satisfy the requirements of this Division. The two regimes serve different purposes. *Corporations Act* registration addresses compliance with corporate law. Social Media Services Register registration addresses accountability for online harms and financial liability to injured third parties. However, a provider's existing local agent may also serve as the nominated Australian entity if that agent meets the requirements of section [X]D.

5.5 Enforcement

The Register itself is an enforcement tool. Service of process on the nominated Australian entity under section [X]D(2)(b) removes the jurisdictional obstacle that currently bedevils litigation against offshore platforms. The Financial Sufficiency Certificate and auditor liability provisions address the separate problem of platforms that submit to jurisdiction but are judgment-proof.

6 Comparison with Precedents

Table 1: Comparison of proposed approach with existing provisions

Feature	Existing Precedent	Proposed provision
Publicly accessible register	*Broadcasting Services Act* s 59: Associated Newspaper Register (maintained by ACMA, publicly available online)	ss [X]A–[X]I: Social Media Services Register (same maintaining authority and public access)
Certified copies admissible as evidence	*Broadcasting Services Act* s 59(7): certified extracts admissible in all courts	s [X]A(5): same rule reproduced
Local agent/address for service	*Corporations Act* ss 601CF–601CJ: mandatory local agent for all registered foreign companies, personally answerable for company's compliance	s [X]D: nominated Australian entity mandatory, capable of suing/being sued; personally liable for damages and penalties (court discretion)
Personal statutory liability of certifier/actuary	*Insurance Act* s 39 and *Life Insurance Act* s 93: Appointed Actuary personally responsible for statutory obligations; APRA's CPS 320 imposes obligations directly on the actuary	s [X]G: certifying auditor personally liable up to certified amount; must maintain PI insurance
Third-party financial surety stepping in on failure	Environmental financial assurance bonds (for example, *Protection of the Environment Operations Act* (NSW) ss 295A–295E): bond surety (bank/insurer) directly liable to regulator if operator fails	s [X]G(2)–(3): auditor "steps into shoes" of provider to extent of certified amount if entity has insufficient funds

7 Contact

Rob Nicholls

Centre for AI, Trust, and Governance

Room L6.04 A14 The Quadrangle
The University of Sydney
NSW 2006

Phone: +61 4 1264 6477

robert.nicholls@sydney.edu.au

ellissa.nolan@sydney.edu.au

sydney.edu.au

https://www.sydney.edu.au/arts/our-research/centres-institutes-and-groups/centre-for-ai-trust-and-governance.html

CRICOS 00026A