Legal 500
Country Comparative Guides 2025

New Zealand
TMT

Contributor

Russell McVeagh

Liz Blythe

Partner, Technology, Digital and Strategic Sourcing | liz.blythe@russellmcveagh.com

Louise Taylor

Special Counsel, Technology, Digital and Strategic Sourcing | louise.taylor@russellmcveagh.com

Craig Shrive

Partner, Public Law and Regulation | craig.shrive@russellmcveagh.com

Tom Hunt

Partner, Banking and Finance | tom.hunt@russellmcveagh.com

Emma Peterson

Partner, Employment | emma.peterson@russellmcveagh.com

This country-specific Q&A provides an overview of tmt laws and regulations applicable in New Zealand.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

New Zealand: TMT

1. Software – How are proprietary rights in software and associated materials protected?

Software can be legally protected in New Zealand in two key ways:

- **Copyright:** Copyright protects original works and arises automatically. The underlying source code or machine-readable translation of the object code of original software may be protected by copyright, under the Copyright Act 1994. The duration of protection depends on the category of the work the copyright subsists in. Copyright can also protect materials associated with the software.
- **Patents:** Following successful application, patents allow the creator of a new invention exclusive use of that invention for up to 20 years and the ability to bring an action against anyone who infringes on that right. Software "as such" is excluded from protection under the Patents Act 2013 if the actual contribution made by the alleged invention lies solely in it being a computer program. However, if the "actual contribution" of the software is part of a redevelopment or improvement of the qualities or features of a machine, the software may be patentable.

2. Software – In the event that software is developed by a software developer, consultant or other party for a customer, who will own the resulting proprietary rights in the newly created software in the absence of any agreed contractual position?

Under the Copyright Act 1994, the person who is the first author of the work is the first owner of any copyright in the work. However, certain exceptions apply under the Copyright Act 1994. Where an author creates a work in the course of their employment, that person's employer is the first owner of any copyright in the work. Similarly, where a person commissions, and pays or agrees to pay for the work, and the work is made in pursuance of that commission, then the person who commissioned the work is the first owner of any copyright in the work. However, it is typically not recommended to rely on default IP ownership laws and IP ownership should be set out clearly in the relevant contract.

3. Software – Are there any specific laws that govern the harm / liability caused by Software / computer systems?

There are no specific laws that govern the harm or liability caused by software or computer systems. However, the following laws apply broadly:

a) Harmful Digital Communications Act 2013: The Harmful Digital Communications Act 2013 applies to online content hosts (including any organisation that hosts websites or social media platforms in New Zealand). Online content hosts may be civilly or criminally liable for the content that is on their website unless they follow a prescribed process, which requires complaints to be received and dealt with in a prescribed way.

b) Crimes Act 1961: Under New Zealand criminal laws, it is an offence to:

i. intend to access, or to access, a computer system dishonestly or by deception;
ii. intentionally or recklessly destroy, damage or alter a computer system knowing, or where one ought to know, that danger to life is likely to result;
iii. intentionally or recklessly and without authorisation:
    a. damage, delete or otherwise interfere with or impair any data or software in a computer system;
    b. cause any of the above to occur; or
    c. cause any computer system to fail, or to deny service to any authorised users; or
iv. make, sell, distribute or process software to assist someone to commit an offence; or
v. access a computer system without authorisation.

These offences are drafted very widely and cover hacking and distributed denial of service. The penalties under these offences range from prison terms of 2 years to a maximum of 10 years.

4. Software – To the extent not covered by (3) above, are there any specific laws that govern the use (or misuse) of software / computer systems?

Please refer to our response in item 3.

5. Software Transactions (Licence and SaaS) – Other than as identified elsewhere in this overview, are there any technology-specific laws that govern the provision of software between a software vendor and customer, including any laws that govern the use of cloud technology?

In New Zealand, there is currently no specific regulatory regime regulating the provision of software between a software vendor and customer, or the use of cloud technology. However, certain New Zealand regulations that apply more broadly also regulate such technology services, such as the Privacy Act 2020, the Unsolicited Electronic Messages Act 2007, and the Fair Trading Act 1986 (as discussed further below).

New Zealand has an unfair contract terms (**UCT**) regime under the Fair Trading Act 1986 with respect to standard form consumer contracts (being business to consumer contracts which aren't generally negotiated) and small trade contracts.

A "small trade contract" under the regime is a standard form contract where the parties are engaged in trade; is not a consumer contract; and does not comprise or form part of a trading relationship that exceeds an annual $250,000 value threshold when the relationship first arises.

A term will be considered "unfair" under the UCT regime if it:

- would cause a significant imbalance in the parties' rights and obligations arising under the contract;
- would cause detriment (whether financial or otherwise) to a party if it were applied, enforced or relied on (with case law indicating that this is a low threshold); and
- is not reasonably necessary in order to protect the legitimate interest of the party who would be advantaged by the term.

Suppliers of technology services and solutions in New Zealand will need to ensure the terms of their standard form consumer contracts and B2B small trade contracts are not in breach of the UCT regime. In particular, the New Zealand regulator, the Commerce Commission, has focussed on unilateral rights of variation and one-sided liability caps/exclusions benefiting the supplier that meet the above criteria as "unfair".

6. Software Transactions (License and SaaS) – Is it typical for a software vendor to cap its maximum financial liability to a customer in a software transaction? If 'yes', what would be considered a market standard level of cap?

It is common for the liability of each party to be subject to a liability cap, with the quantum of that liability cap varying depending on the circumstances. For the supply of "off-the-shelf" software solutions, suppliers commonly seek to cap their liability at 100% of fees paid in a 12-month period. The liability provisions in contracts for the supply of bespoke or business critical solutions are commonly negotiated.

In New Zealand, the Courts will generally enforce liability clauses where they are negotiated at arm's length between commercial parties. However, there is scope, under the Fair Trading Act 1986, for challenging the enforceability of liability provisions in standard form contracts if one of the parties is a "consumer" or if the annual value of the trading relationship is less than NZD250,000 (as discussed above in item 5).

7. Software Transactions (License and SaaS) – Please comment on whether any of the following areas of liability would typically be excluded from any financial cap on the software vendor's liability to the customer or subject to a separate enhanced cap in a negotiated software transaction (i.e. unlimited liability): (a) confidentiality breaches; (b) data protection breaches; (c) data security breaches (including loss of data); (d) IPR infringement claims; (e) breaches of applicable law; (f) regulatory fines; (g) wilful or deliberate breaches.

It is common in New Zealand for software customers to seek to include certain key uncapped heads of loss in the contract, such as: breach of confidentiality; breach of the provisions relating to intellectual property rights (including third party IPR infringement claims on an indemnity basis); wilful or deliberate breaches; and fraud.

In addition, if the software vendor will have access to personal information of the customer, customers are increasingly seeking uncapped liability, or a separate higher cap, for the software vendor's breach of its data protection and security obligations.

8. Software Transactions (License and SaaS) – Is

it normal practice for software source codes to be held in escrow for the benefit of the software licensee? If so, who are the typical escrow providers used? Is an equivalent service offered for cloud-based software?

Software escrow arrangements are only typically at the licensee's request and only where the software vendor is providing business critical (and often bespoke or customised) software to a customer with significant bargaining power in circumstances where alternative solutions are not readily available in the market and/or the time to procure and implement an alternative solution would expose the licensee to significant business risk. Escrow arrangements are more common in licence transactions than SaaS arrangements, but are becoming increasingly uncommon overall. They are now unusual in a SaaS context, except where the software is being used in high-risk, regulated applications. Escrow NZ is New Zealand's most commonly used escrow provider.

9. Software Transactions (License and SaaS) – Are there any export controls that apply to software transactions?

No.

10. IT Outsourcing – Other than as identified elsewhere in this questionnaire, are there any specific technology laws that govern IT outsourcing transactions?

Outsourcing transactions are not separately regulated in New Zealand. Rather, whether or not a particular outsourcing arrangement will be the subject of a specific regulatory regime will largely depend on the customer's industry and the specific nature of the arrangement. For example, in New Zealand, large banks must comply with the Reserve Bank of New Zealand's BS11 Outsourcing Policy in respect of certain outsourcing arrangements.

While not relating to outsourcing specifically, New Zealand's competition law, the Commerce Act 1986 (**Commerce Act**) contains prohibitions against cartel agreements between competitors. Namely, it is illegal "cartel conduct" for competing businesses to agree:

- what prices each will charge customers in competition with each other (known as "price fixing");
- what customers or territories each will supply, or will not supply, in competition with each other (known as "market allocation"); and
- to not supply certain goods or services in competition with each other (known as an "output restriction agreement").

These prohibitions could apply to an outsourcing agreement where the provider of the relevant services is also a competitor of the customer of those services. Illegal conduct can be found without a written agreement and an informal expectation between competitors that they will act in a certain way is sufficient to breach the Commerce Act. Therefore, discussions with outsourcing partners that are also competitors should not "spillover" into informal understandings as to how each competes for customers and the parties should avoid sharing commercially sensitive information (such as pricing information) with each other in the areas in which they compete.

The Commerce Act contains an exemption from the cartel prohibition for clauses included in supply contracts (such as an IT outsourcing contract), provided those clauses do not have the purpose of lessening competition between the parties. This is increasingly an area to watch in New Zealand as IT service providers are, more and more, outsourcing their own IT operations to outsourced service providers who may also be competitors in some markets.

11. IT Outsourcing – Please summarise the principal laws (present or impending), if any, that protect individual staff in the event that the service they perform is transferred to a third party IT outsource provider, including a brief explanation of the general purpose of those laws.

New Zealand's transfer regime for employees in outsourcing scenarios only applies for particular work (cleaning, food catering and security) so does not apply in relation to an outsourcing to an IT provider. However, the outsourcing would likely lead to the termination of employment with the existing provider. The new provider may (but is not required to at law) offer employment. If employment is offered by the new provider, it may be on terms decided by the new provider (there is no obligation at law to offer the same terms and conditions of employment).

Where the work of an employee is to move to another provider, the employer is required to consult with the employee prior to making a decision to outsource the work. This is the main protection provided to individual staff members in the event the service they perform is outsourced to a third party. A compliant consultation

process is generally structured as follows:

- the employer provides all relevant information regarding the proposed outsourcing decision, including whether the employee's role could be disestablished and employment terminated;
- the employee is given an opportunity to consider the information provided and formulate a response;
- the employee provides that response to the employer;
- the employer genuinely considers the employee's feedback; and
- the employer then makes a decision regarding whether to outsource the work as proposed. If the work is to be outsourced, further consultation would occur regarding the impact on the employee (i.e. are there any alternatives to redundancy).

The general purpose of these provisions is to ensure that employees have an opportunity to provide feedback into decisions that affect the continuity of their employment.

12. Telecommunications – Please summarise the principal laws (present or impending), if any, that govern telecommunications networks and/or services, including a brief explanation of the general purpose of those laws.

Under the Telecommunications Act 2001 ("**Telecommunications Act**"), the key regulatory regimes can be summarised as follows:

- Regulation of fixed fibre lines services. Chorus, the main provider in New Zealand, is subject to price-quality regulation. Other providers are subject to information disclosure. There are powers to allow price regulation of specific services provided over fibre. Providers are also subject to enforceable Deeds with the Crown which require them to provide services on an equivalence of inputs and/or non-discriminatory basis.
- Access regulation of copper lines services. Some broadband services remain subject to standard terms determinations, which govern the prices and terms on which the services are provided to access seekers. There is a regime governing the withdrawal of coppers services as and when they are replaced by fibre.
- Regulation of some aspects of mobile services. For example, mobile termination access services are subject to price regulation, and mobile co-location services are subject to access (but not price) regulation.
- Line of business restrictions. Chorus must not enter the retail market.
- A general power for the Commission to undertake market studies. For example, it has reviewed issues that could inhibit mobile market development, and has undertaken a review of rural connectivity services.
- Consumer protection. This includes the ability for the Commission to prescribe industry codes (such as the 111 contact code and retail service quality code) and undertake retail market monitoring.
- A property and road / rail corridor access regime for network operators.

The Telecommunications (Interceptions Capability and Security) Act 2013 (**"TICSA"**) applies to network operators (lines and mobile) and governs:

- Obligations to ensure networks have interception capability and duties to cooperate with law enforcement and surveillance agencies;
- Requirements for network security, including engagement with the Government Communications Security Bureau on security risks and network changes that could impact security.

13. Telecommunications – Please summarise any licensing or authorisation requirements applicable to the provision or receipt of telecommunications services in your country. Please include a brief overview of the relevant licensing or authorisation regime in your response.

There are no licencing requirements for the supply or receipt of telecommunications services.

Under the Telecommunications Act 2001, telecommunications providers may apply to be declared a "network operator" for the purposes of the Telecommunications Act, though it is not mandatory.

Under TICSA a person who controls or operates a public telecommunications network or supplies another person with the capability to provide a telecommunications service constitutes a "network operator". TICSA requires network operators to register on the register of network operators maintained by the New Zealand Police.

TICSA also requires network operators to notify the Director-General of the Government Communications Security Bureau (**"Director-General"**) (**"Bureau"**) of proposed decisions, courses of action or changes regarding certain parts of their network. Only proposals affecting an "area of specified security interest" need to be notified. An "area of specified security interest" means –

- network operations centres;
- lawful interception equipment or operations;
- any part of a public telecommunications network that manages or stores aggregated information or authentication credentials of a significant amount of customers;
- any place in a public telecommunications network where data belonging to a customer or end user aggregates in large volumes; and
- any area prescribed by the Governor-General by Order in Council.

Additionally, network operators must engage, in good faith, with the Bureau if they become aware that the implementation of any other decision, course of action, or change to any part of their network may give rise to a network security risk.

Notifications will be subject to assessment by the Director-General, or if the case requires, the Minister responsible for the Bureau. If a network security risk is identified, then the action, decision or change must not be implemented unless the Director has accepted a proposal to mitigate the risk or directions by the Minister are complied with.

14. Telecommunications – Please summarise the principal laws (present or impending) that govern access to communications data by law enforcement agencies, government bodies, and related organisations. In your response, please outline the scope of these laws, including the types of data that can typically be requested, how these laws are applied in practice (e.g., whether requests are confidential, subject to challenge, etc.), and any legal or procedural safeguards that apply.

Government agencies, including police and other law enforcement agencies, commonly make requests for personal information from other various agencies.

The Intelligence and Security Act 2017 ("**Security Act**") provides the legislative regime for the New Zealand Security Intelligence Service and the Government Communications Security Bureau. The Security Act provides for these agencies to request information from other agencies in situations where they have a reasonable belief that this information is necessary for the performance of its functions. Both the Security Act and the Search and Surveillance Act 2012 contain provisions relating to obtaining information through search warrants and production orders.

TICSA contains obligations on network operators to ensure that their networks have interception capability. Such capability requires that surveillance agencies lawfully authorised to intercept will be able to intercept telecommunications on the network unobtrusively and obtain call associated data and content of telecommunications in a usable format.

Additionally, when presented with a lawful authority to intercept (by a surveillance agency), network operators and service providers are under a duty to assist. This requires making officers and employees available to provide technical assistance and / or taking other reasonable steps necessary to give effect to the warrant or lawful authority such as assisting with the lawful interception itself.

15. Mobile communications and connected technologies – What are the principle standard setting organisations (SSOs) governing the development of technical standards in relation to mobile communications and newer connected technologies such as digital health or connected and autonomous vehicles?

There are currently no SSOs or specific regulatory regimes governing the overall setting of technical standards in relation to mobile communications. In New Zealand, mobile network operators develop and maintain the standards that must be met for them to consent to connection to their networks.

Radio Spectrum Management administers the radiocommunications regime in New Zealand. Regulations and notices under that regime establish a product compliance framework, including designating the performance standards that apply to all electrical, electronic and radio products. The applicable standards are outlined in the Radiocommunications (EMC Standards) Notice 2019 and Radiocommunications (Radio Standards) Notice 2023.

Industries using connected technologies in New Zealand may also develop and manage their own standards. For example, Te Whatu Ora – Health New Zealand has established its own Health Information Standards Organisation, which sets non-binding data and digital standards for New Zealand's health sector in line with international standards.

16. Mobile communications and connected technologies – How do technical standards facilitating interoperability between connected devices impact the development of connected technologies?

Technical standards facilitating interoperability in New Zealand are relatively limited and do not impact the development of connected technologies to any greater extent than applicable overseas standards.

17. Data Protection – Please summarise the principal laws (present or impending), if any, that govern data protection, including a brief explanation of the general purpose of those laws.

The Privacy Act 2020 regulates the collection and processing of personal information. The purpose of the Privacy Act 2020 is to promote and protect individual privacy by:

- providing a framework for protecting an individual's right to privacy of personal information, including the right of an individual to access their personal information, while recognising that other rights and interests may at times also need to be taken into account; and
- giving effect to internationally recognised privacy obligations and standards in relation to the privacy of personal information, including the OECD Guidelines and the International Covenant on Civil and Political Rights.

The Office of the Privacy Commissioner has also issued several codes of practice pursuant to the Privacy Act 2020, which become part of the law. These include codes in the areas of civil defence, credit reporting, health information, justice sector unique identifiers, superannuation scheme unique identifiers, and telecommunications information. A new Biometric Processing Privacy Code is also currently being prepared by the Office of the Privacy Commissioner (as described in more detail in item 23 below).

18. Data Protection – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable data protection laws?

The maximum fine under the Privacy Act 2020 is NZ$10,000. This is for a range of offences, including failure to comply with an access order, compliance notice or transfer prohibition notice, and failure to notify a privacy breach where required under the Privacy Act 2020.

19. Data Protection – Do technology contracts in your country typically refer to external data protection regimes, e.g. EU GDPR or CCPA, even where the contract has no clear international element?

Technology contracts in New Zealand typically require both parties to comply with the Privacy Act 2020 at a minimum. This applies even if the software vendor is EU GDPR, UK GDPR or CCPA compliant. The Privacy Act 2020 has a similar standard to the EU GDPR in some areas, including in respect of cross border transfers of personal information and mandatory breach reporting. However, in other areas a more permissive standard than the EU GDPR's prescriptive requirements apply. This usually means that if a software vendor is EU or UK GDPR compliant, then it is likely that they will be Privacy Act 2020 compliant as well in most areas.

If the customer provides the software vendor with personal information of European Union or United Kingdom residents, then customers may require the supplier to be EU GDPR and/or UK GDPR compliant in addition to Privacy Act 2020 compliance.

20. Cybersecurity – Please summarise the principal laws (present or impending), if any, that govern cybersecurity (to the extent they differ from those governing data protection), including a brief explanation of the general purpose of those laws.

The New Zealand Cybersecurity Strategy 2019, while not law, outlines New Zealand's priorities for improving cybersecurity for individuals, businesses and government agencies alike, through cybersecurity awareness, resilience, proactiveness and involvement in international discussion.

In New Zealand, specific cybercrime is broadly criminalised under the Crimes Act 1961, as discussed in item 3. Additionally, while there is no principal regulation governing cybersecurity, certain New Zealand regulations which apply to components of cybersecurity such as data protection and network security, also apply more broadly to cybersecurity. For example, provisions under the Privacy Act 2020 including the requirement for agencies to protect personal information from loss, access, misuse

and modification, and as discussed at item 13, provisions under TICSA that require notification and engagement with the Bureau on network security risks.

New Zealand's cyber-security agency, the National Cyber Security Centre, which is part of the Bureau, targets cybersecurity at a national level through its protection of New Zealand's critical infrastructure from cyber threats.

21. Cybersecurity – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable cybersecurity laws?

The maximum sentence for a breach of the Crimes Act 1961 cybercrime provisions (sections 248 – 252) is a term of 10 years imprisonment (see item 3). Failure to comply with the Privacy Act 2020 provisions can lead to fines of NZD10,000 per offence, notably for failures to report data breaches. Fines under TICSA can reach a maximum of NZD500,000.

22. Artificial Intelligence – Which body(ies), if any, is/are responsible for the regulation of artificial intelligence?

There is no specific regulator of artificial intelligence (**AI**) in New Zealand. However, relevant laws that apply more broadly are regulated by the Office of the Privacy Commissioner and the Commerce Commission.

23. Artificial Intelligence – Please summarise the principal laws (present or impending), if any, that govern the deployment and use of artificial intelligence, including a brief explanation of the general purpose of those laws.

In New Zealand, there is currently no specific regulatory regime that regulates artificial intelligence (**AI**) but certain New Zealand legislation that applies more broadly to technology will apply to AI including the Privacy Act 2020, Human Rights Act 1993, and the Fair Trading Act 1986.

The Government released an Algorithm Charter (**Charter**) in July 2020, which (among other things) requires signatory public agencies to use algorithms in an ethical, trustworthy way. The Algorithm Charter applies only to public sector agencies that have signed up to it.

The Office of the Privacy Commissioner (**OPC**) is currently preparing to issue a Biometric Processing Privacy Code (**Biometrics Code**). The Biometrics Code will apply to agencies that collect and use biometric information (such as fingerprints or facial images) to verify, identify or categorise individuals using automated processing. However, it will not apply to the biometric processing activities of health agencies or biometric information collected or held by health agencies, and there are some limited exceptions for intelligence and security agencies. The Privacy Commissioner has indicated that a final version of the Biometrics Code will be issued mid-2025.

The New Zealand Government has indicated that it has a low appetite for AI-specific regulation in New Zealand. In a Cabinet Paper dated 25 July 2024 the current Government stated that it will take a "light-touch, proportionate and risk-based approach" to AI regulation. The Government confirmed this approach in its National AI Strategy, which was released in July 2025. Accordingly, it is expected that there will be very limited AI-focused regulation in New Zealand in the near future (if any).

The Government has also recently released "Responsible AI Guidance for the Public Service" and a "Public Sector AI Framework" to support public sector agencies in using AI. The guidance builds on the interim public sector guidance released in 2023 and, alongside the Public Service AI Framework, forms part of the National AI Strategy mentioned above. In July 2025, the Government also released Responsible AI Guidance for Businesses to provide guidance in the private sector on a voluntary basis.

24. Artificial Intelligence – Are there any specific legal provisions (present or impending) in respect of the deployment and use of Large Language Models and/or generative AI (including agentic AI)?

There is no specific regulatory regime that regulates generative AI. However, the comments at item 23 will also apply to generative AI. In addition, the Office of the Privacy Commissioner has released practical guidance on the use of generative AI by New Zealand organisations. While the guidance is limited to generative AI, it is also relevant to the use of other AI tools.

25. Artificial Intelligence – Do technology contracts in your jurisdiction typically contain either mandatory (e.g. mandated by statute) or recommended provisions dealing with AI risk? If so, what issues or risks need to be addressed or considered in such provisions?

There are currently no mandatory provisions dealing with AI-specific risks in New Zealand. Customers of AI systems in New Zealand will generally expect the supplier to provide assurances in respect of key AI risks such as bias, copyright infringement, human oversight and transparency. Contracts also typically deal with other key matters such as privacy and data protection, adherence to specifications or published documentation, and IP ownership in outputs. However, whether technology contracts relating to AI systems address AI-specific risks will depend on a range of factors including the nature of the AI system and its intended use.

26. Artificial Intelligence – Do software or technology contracts in your jurisdiction typically contain provisions regarding the application or treatment of copyright or other intellectual property rights, or the ownership of outputs in the context of the use of AI systems?

Technology contracts dealing with AI systems in New Zealand typically address the ownership of intellectual property rights in the AI system and in the output produced by the AI system. The supplier will typically retain rights in the underlying AI system unless it has been commissioned as a bespoke offering for the customer. The customer will typically own the output of an AI system and be responsible for its use (including compliance with applicable laws in connection with such use). However, this position varies depending on various factors including those discussed at item 25.

27. Blockchain – What are the principal laws (present or impending), if any, that govern (i) blockchain specifically (if any) and (ii) digital assets, including a brief explanation of the general purpose of those laws?

New Zealand lacks targeted legislation that governs blockchain or digital assets alone. Instead, digital assets and services related to digital assets in New Zealand are regulated by existing, technology neutral legislation. Given that the rights and functions created in respect of digital assets are flexible, each asset or service associated with digital assets will be regulated according to its specific properties. The two regimes most relevant to blockchain and digital assets are those which govern financial products under the FMCA and the AML/CFT Act.

The FMCA is the principal piece of legislation that regulates financial products. The FMCA:

- imposes fair dealing obligations on conduct in both the retail and wholesale financial markets;
- sets out the disclosure requirements for offers of financial products;
- set out a regime of exclusions and wholesale investor categories in connection with the disclosure requirements;
- set out the governance rules that apply to financial products; and
- impose licensing regimes.

Whether the more onerous requirements of the FMCA apply in relation to a specific digital asset depends on whether that digital asset meets the definition of "financial product" as set out in the FMCA.

The AML/CFT Act sets out a range of anti-money laundering obligations (such as customer due diligence) which applies to reporting entities. The definition of reporting entity includes virtual asset service providers, which means that service providers in relation to digital assets are typically subject to obligations under that legislation. The primary purpose of that legislation is to deter and detect money laundering and the financing of terrorism.

28. Search Engines and Marketplaces – Please summarise the principal laws (present or impending), if any, that govern search engines and marketplaces, including a brief explanation of the general purpose of those laws.

There is no specific regulation of search engines and marketplaces. General consumer protection and privacy laws apply (e.g. Fair Trading Act 1986, Consumer Guarantees Act 1993, and the Privacy Act 2020 and Privacy Regulations 2020).

New Zealand consumer law applies to goods or services provided to people in, or business carried out in, New Zealand. The Commerce Commission can regulate such activities, and in doing so can initiate enforcement action against residents of other countries. The Privacy Act 2020 is discussed above.

The Harmful Digital Communications Act 2013, as discussed in item 3, applies to online content hosts (including any organisation that hosts websites or social media platforms in New Zealand). Online content hosts may be civilly or criminally liable for the content that is on their website unless they follow a prescribed process, which requires complaints to be received and dealt with in a prescribed way.

In 2019, New Zealand developed the Christchurch Call, which is an action plan that commits government and tech companies to a range of measures in an attempt to make the internet safer. This includes developing tools to prevent the upload of violent content and increasing transparency around the removal and detection of content. The Christchurch Call is not binding, and there are no legal consequences for parties that fail to comply.

29. Social Media – Please summarise the principal laws (present or impending), if any, that govern social media and online platforms, including a brief explanation of the general purpose of those laws?

Our comments in relation to search engines and marketplace in item 28 also apply to social media.

30. Social Media – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable online safety laws?

Sanctions under general consumer protection and privacy laws can differ greatly depending on the relevant provision breached. Under the Harmful Digital Communications Act 2013, a person who causes harm by posting digital communication is liable on conviction to imprisonment for up to 2 years or a fine up to NZD50,000 in the case of an individual, or a fine up to NZD200,000 in the case of a body corporate.

31. Spatial Computing – Please summarise the principal laws (present or impending), if any, that govern spatial computing, including a brief explanation of the general purpose of those laws?

There are no specific regulations pertaining to spatial computing in New Zealand.

32. Quantum Computing – Please summarise the principal laws (present or impending), if any, that govern quantum computing and/or issues around quantum cryptography, including a brief explanation of the general purpose of those laws?

There are no specific regulations pertaining to quantum computing in New Zealand. However, given that quantum computing has the potential to compromise cryptographic systems, existing legislation such as the Crimes Act 1961 and the Privacy Act 2020 will likely have application to issues created by quantum computing and cryptography.

33. Datacentres – Does your jurisdiction have any specific regulations that apply to data centres?

New Zealand does not have legislation that specifically applies to datacentres. However, due to the importance of data sovereignty, general information protection regulations under the Privacy Act 2020, as discussed at item 17 above, apply more broadly to datacentres.

TICSA also has limited application to datacentres. Datacentres that provide / make available telecommunications services are considered "service providers" under TICSA and therefore, when required, must assist with the lawful interception of telecommunications.

The International Organization for Standardization's ("**ISO**") international standard 27001 guides best practice for information security management. While adherence to this standard provides credibility for datacentres, it is not mandatory.

34. General – What are your top 3 predictions for significant developments in technology law in the next 3 years?

Our top 3 predictions for significant developments in technology law in New Zealand in the next 3 years are as follows:

a. **New legislation:** New legislation currently being considered by the Government and certain new legislation that has recently come into effect may have a significant impact on technology law in New Zealand:
    i. **Customer and Product Data Act:** The Customer and Product Data Act ("**Act**") was passed into law and came into force in March 2025 – forming New Zealand's consumer data right (CDR) framework. Once implemented, the CDR will provide individuals and businesses with a statutory ability to require data holders to share information held about them with trusted third parties and the ability to require them to carry out some form of action on the relevant individual's or

businesses' behalf. The Government has confirmed that the banking sector will be the first sector to be designated in-scope of the CDR and has consulted on whether the electricity sector should be designated next. The Ministry of Business, Innovation and Employment has confirmed that the banking regulations to be issued under the Act are expected to be in force from December 2025.

ii. **Digital Identity Trust Framework:** The Digital Identity Trust Framework Act 2023 (**Act**) will impact the provision and receipt of digital identity services in New Zealand. The core objective of the Act is to help develop digital identity services that are trusted and people-centric. While the primary obligations in the Act will be on digital identity service providers on an opt-in basis, it will also have an impact on individuals and organisations in the digital identity ecosystem, including banks, government agencies, utility and telecommunications providers. The rules that will apply to digital identity service providers who opt-in to the framework are still in development.

b. **Regulation of Biometrics:** The Office of the Privacy Commissioner (**OPC**) is expected to release a final version of the Biometrics Code mid-2025. Refer to our comments at item 23.

c. **AI roadmap/risk management:** As part of the National AI Strategy, the New Zealand Government released the "Responsible AI Guidance for the Public Service: GenAI" to assist public sector agencies in using AI in a safe and responsible way, as discussed at item 23. The Government also released private sector guidance in July 2025 (as discussed at item 23). While non-binding, both sets of guidance are likely to be influential on industry standards in the public and private sectors. Both sets of guidance reflect a low appetite for regulating AI in New Zealand, encourage the adoption and use of AI by New Zealand organisations, and clarify the Government's expectations in terms of key considerations when using and implementing AI systems.

35. General – Do technology contracts in your country commonly include provisions to address sustainability / net-zero obligations or similar environmental commitments?

Yes. Organisations that are subject to net-zero obligations or environmental commitments under law or internal policies may request their suppliers to comply with certain environmental, social and governance (ESG) requirements.

Contributors

Liz Blythe
Partner, Technology, Digital and Strategic Sourcing
liz.blythe@russellmcveagh.com

Louise Taylor
Special Counsel, Technology, Digital and Strategic Sourcing
louise.taylor@russellmcveagh.com

Craig Shrive
Partner, Public Law and Regulation
craig.shrive@russellmcveagh.com

Tom Hunt
Partner, Banking and Finance
tom.hunt@russellmcveagh.com

Emma Peterson
Partner, Employment
emma.peterson@russellmcveagh.com