IN-DEPTH

Privacy, Data Protection and Cybersecurity

EDITION 10

Contributing editor
Alan Charles Raul
Sidley Austin LLP

LEXOLOGY

Published in the United Kingdom
by Law Business Research Ltd
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK

www.thelawreviews.co.uk

ISBN 978-1-80449-214-7

Acknowledgements

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

ANDERSON LLOYD

ANJIE BROAD LAW FIRM

BOMCHIL

CHRISTOPHER & LEE ONG

CLEMENS LAW FIRM

CTSU, SOCIEDADE DE ADVOGADOS, SP, RL, SA

GREENBERG TRAURIG LLP

JACKSON, ETTI & EDU

KALUS KENNY INTELEX

KPMG CHINA

LECOCQASSOCIATE

LEE, TSAI & PARTNERS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

Chapter 14

NEW ZEALAND

Derek Roth-Biester, Megan Pearce and Emily Peart[1]

I OVERVIEW

The key legislation in New Zealand governing privacy and data protection is the Privacy Act 2020 (Privacy Act). The Privacy Act repealed and replaced its predecessor legislation, the Privacy Act 1993, with most operative provisions of the new Act coming into force on 1 December 2020.

The Privacy Act retains the technology-neutral, principle-based approach contained within the former legislation and strengthens the Act's privacy protections by promoting early intervention and privacy risk management by agencies[2] (including by introducing a mandatory privacy breach notification regime).

The implementation of the Privacy Act followed a long period of review that coincided with significant developments in the use of data-centric technologies and strengthening of international data protection regulation. There remains ongoing debate as to whether the new Act went far enough to drive best privacy practice, particularly in the context of the rapid release and application of AI generative tools, biometric and other data-centric technologies, given that monetary penalties under the Act remain light when compared to the GDPR and data protection laws in many other comparable jurisdictions.

In 2012, New Zealand was one of the first jurisdictions to be recognised by the European Commission (EC) as having 'adequacy status' – meaning that New Zealand was deemed to meet European legal standards of data protection (facilitating the free flow of personal information from EU countries to New Zealand for processing). Following Brexit, the UK equivalent of the GDPR recognised New Zealand's adequacy status – permitting the continued free flow of personal information between the UK and New Zealand. While at present New Zealand retains its adequacy status, New Zealand's status remains under review by EU officials following the implementation of the Privacy Act.[3]

There is no single piece of dedicated legislation regulating cybersecurity and cybercrimes in New Zealand. The Privacy Act deals with cybersecurity only in relation to personal information (discussed further in Section IX). The Intelligence and Security Act 2017 separately regulates state-based surveillance and provides for the establishment of the Government Communications Security Bureau (GCSB), whose role includes supporting

1 Derek Roth-Biester is a partner, Megan Pearce is a senior associate and Emily Peart is a solicitor at Anderson Lloyd.

2 An agency is the name used by the Privacy Act for organisations and persons processing personal information to whom the Privacy Act applies.

3 https://www.justice.govt.nz/justice-sector-policy/regulatory-stewardship/regulatory-systems/civil-law/privacy/.

the response to cybersecurity incidents impacting New Zealand's nationally significant organisations. Limited cyber-related offences are also provided for the Crimes Act 1961 in respect of crimes involving computers and computer systems, while entities that are regulated by the Financial Markets Authority (including financial service and advice providers) or the Reserve Bank (RBNZ) (including banks, non-bank deposit takers and insurers) are subject to separate, sector-specific guidance in relation to cyber resilience.

II THE YEAR IN REVIEW

i Generative artificial intelligence

The past 12 month has seen the rapid release of generative artificial intelligence (AI) tools directly to consumers, including OpenAI's ChatGPT, Microsoft's Bing search or Copilot products and Google's Bard. Widespread adoption of such generative AI tools has seen regulators across the globe deliberating appropriate regulation of these technologies and how best to fill the gaps present in existing data protection and privacy laws. In New Zealand, the Privacy Commissioner (the Commissioner) has acknowledged that while the Privacy Act is technology-neutral and already applies to AI, further discussion is needed both domestically and internationally regarding what we want AI to do and what limitations are necessary. The Commissioner further emphasised that the conversation (regarding regulation of AI technologies) is becoming more urgent as private developers release more advanced and competing AIs, and it will require a collective response from the public sector and private businesses.

Dedicated legislation specifically regulating AI has not yet been enacted in New Zealand, however, the Privacy Act will apply to the use of generative AI tools to the extent those tools process personal information. In June 2023, the Commissioner released guidance regarding the Office of the Privacy Commissioner (OPC)'s expectations concerning the use of generative AI[4] (further discussed in Section V.v). New Zealand has also recently seen sectoral efforts to promote responsible AI governance through issuing best practice standards. An example of this the Algorithm Charter for Aotearoa, a 'soft law' instrument, which is a commitment by New Zealand's government agencies to ensure their use of AI strikes the balance between respecting individuals' privacy, transparency and the efficiencies that AI has to offer.[5]

ii Implementation of a consumer data right

A consumer data right (CDR) is generally accepted to be statutory right for consumers to share data held about them by agencies with third parties. A CDR provides consumers with wide-ranging benefits, including increased competition.

The Privacy Act did not introduce a CDR despite the then Commissioner's recommendation for this in his submissions on the Privacy Bill.[6] However, in June 2023, the Ministry of Business, Innovation and Employment (MBIE) opened a consultation on the

4 https://www.privacy.org.nz/publications/guidance-resources/generative-artificial-intelligence-15-june-2023-update/#:~:text=The%20Privacy%20Act%20is%20technology,information%20via%20paper%20or%20computer).

5 Stats NZ Tatauranga Aotearoa, 'Algorithm Charter for Aotearoa New Zealand' (2020), 1.

6 Privacy Commissioner, 'Submission on the Privacy Bill to the Justice and Electoral Select Committee' (31 March 2018).

exposure draft of the Customer and Product Data Bill (the CDR Bill).[7] The CDR Bill relies on the existing protections and data security safeguards under the Privacy Act.[8] For example, 'customer data' requests under the CDR Bill reflect the right for individuals to request access to their personal information as set out in the Privacy Act; however, the intent behind the drafting of these requests under the CDR Bill is to specifically enable these requests to be handled in a standardised process enabling the data to be transported easily from one system to another. The OPC will continue to exercise jurisdiction over privacy-related issues under the CDR Bill.

iii Cybersecurity

Malicious cyberactivity in New Zealand continues to largely align with international trends, seeing rapid increases in the use of ransomware and exploitation of internet-facing services and applications. New Zealand's National Cyber Security Centre (NCSC) reported two highly significant incidents affecting New Zealand's nationally significant organisations during the 1 July 2021 to 30 June 2022 year (discussed further in Section IX).[9]

However, regulation of cybersecurity and cyber-related incidents in New Zealand continues to be fragmented. Given the development of prescriptive cybersecurity legislation in Australia, we stand by to see whether there is any flow-on effect for regulation in New Zealand.[10]

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The Privacy Act[11] governs how agencies subject to the Act may collect, store, use and share personal information.[12] The Act applies to 'agencies', which captures New Zealand residents, most public and private sector New Zealand organisations as well as overseas organisations in respect of actions taken while carrying on business in New Zealand.[13]

The Privacy Act contains 13 information privacy principles (IPPs) which provide the framework governing how agencies may collect, handle and use personal information. The Act does not distinguish between different classes of personal information, for example, by providing for specific rules relevant to 'sensitive' personal information or similar. However, the Act does provide that the Commissioner may issue codes of practice under the Act which may modify the application of the IPPs and set privacy rules relevant to specific classes of information, industry sectors or classes of agency subject to the Act.[14]

7 Ministry of Business, Innovation and Employment (MBIE), 'Customer and Product Data Bill'.

8 Ministry of Business, Innovation and Employment (MBIE), 'Unlocking value from our customer data – discussion document' (June 2023), 17.

9 National Cyber Security Centre, 'Cyber Threat Report 2021/22', 6.

10 Australian Government, '2023-2030 Australian Cyber Security Strategy Discussion Paper', (February 2023).

11 Privacy Act 2020.

12 Personal information being broadly defined under the Privacy Act as information of about an identifiable natural person (other than a deceased natural person).

13 Privacy Act, Section 4.

14 id., Section 32.

The Act does not distinguish between 'data controllers' and 'data processors' other than to note that where an agency (Agency A) holds personal information as an agent for another agency (Agency B) – for example, for safe custody or processing (irrespective of where Agency A is located) – then the information is treated as being held by Agency B unless Agency A also uses or discloses the information for its own purposes.[15]

When compared to many overseas jurisdictions, penalties under the Privacy Act are light. Under the Privacy Act, penalties of up to NZ$10,000 can be imposed for failure to comply with certain provisions of the Act, including failure to comply with an access order issued by the Commissioner, failure to notify the Commissioner of a notifiable privacy breach and failure to comply with any lawful requirement of the Commissioner under the Act.

The Commissioner has broad powers to investigate privacy complaints, make binding decisions on access requests and to issue compliance notices directing agencies to start or stop doing something to comply with the Privacy Act or a code of practice. Only one compliance notice has been issued by the Commissioner since the introduction of the regime in December 2020 (discussed further in Section VII).

If a complaint has been investigated by the Commissioner, the Privacy Act gives aggrieved individuals the right to file a claim in the Human Rights Review Tribunal (the Tribunal). The Tribunal can award compensatory damages for losses suffered up to NZ$350,000. See Section VII for more details on recent Tribunal decisions relating to complaints arising under the Privacy Act.

ii General obligations for data handlers

Collection of personal information

IPP1 provides that agencies may only collect personal information if the information is collected for a lawful purpose connected with a function of the agency and the collection of the information is necessary for that purpose. If the purpose for which information is collected does not require that collection then the agency may not require that information.[16]

IPP1 does not go so far as to require the collection of the personal information to be the only way to achieve the agency's relevant purpose. However, agencies must have a clear and reasonably justifiable purpose for each collection of personal information.

As a general rule, personal information must be collected directly from the person to whom it relates. However, agencies may collect personal information other than from the individual concerned in prescribed circumstances[17] including where the agency believes on reasonable grounds that direct collection would prejudice the purposes of the collection (i.e., collection via CCTV for the purposes of security monitoring).

Where personal information is collected directly, the collecting agency must take reasonable steps to ensure that the individual concerned is aware of certain prescribed matters. These prescribed matters include:

a the purpose for which the information is being collected;

b the intended recipients of the information;

c details of the agency collecting that information and the agency that will hold the information;

15 id., Section 11.

16 id., Section 22 (IPP1).

17 id. (IPP2).

d if the collection of the individual's information is required by law; and
e the individual's rights of access to, and correction of, their information.[18]

The government is considering an expansion to the Privacy Act's current notification rules, specifically, whether the notification regime should also apply to agencies when collecting personal information indirectly via third parties. Public submissions on the proposed change closed in September 2022, and the government is currently considering responses to determine whether changes to notification regime are required.

Use and disclosure of personal information

Agencies may only use and disclose personal information:

a with consent;
b for the purpose for which the information was collected;
c for a purpose directly related to the purpose in connection with which the information was obtained; or
d if another prescribed exception applies (i.e., where the use or disclosure is necessary to prevent a serious threat to public health or public safety).

In practice, this means that agencies wishing to use or disclose personal information for a purpose beyond the purposes for which the information was originally collected (each a primary purpose) must take steps to obtain the individual's consent to that further use or disclosure or ensure that further use or disclosure is directly related to the primary purposes (such that the individual would reasonably anticipate the agency's further use or disclosure of their information).

Storage and security of personal information

All agencies that hold personal information must ensure that the information is protected by reasonable security safeguards against loss or unauthorised access, use, modification or disclosure (discussed further in Section IX).[19]

Agencies are also restricted from retaining personal information for longer than is required for the purposes for which the information may lawfully be used (i.e., the purposes originally disclosed at the time of collection or any subsequent consented purpose).

Compliance with data subject rights

Agencies that hold personal information must comply and respond to an individual's requests for access to and correction of that information in accordance with the processes prescribed in the Privacy Act (discussed further in Section III.iii).

18 id. (IPP3).
19 id. (IPP5).

iii Data subject rights

Access and correction

Individuals have the right to request access to and correction of their personal information. Agencies must comply with these requests within prescribed time frames subject to certain exceptions (i.e., where the disclosure of the information would be likely to pose a serious threat to the life, health or safety of any individual, or to public health or public safety).[20]

Erasure

There is no express right to erasure in New Zealand; however, it is arguable in certain circumstances that as individuals may request their information to be corrected, the required correction may involve deletion of that information.

Under the Harmful Digital Communications Act 2015, individuals who suffer harm caused through digital communications (i.e., online posts, text messages) may apply to the courts for removal of the offending material. Successful applications may result in court orders against the offending individual or the relevant online content host to take down the offending material.

Data portability

There is currently no express right of data portability in New Zealand. However, in June 2023 the government released an exposure draft of the CDR Bill introducing a statutory right to require data holders to securely share personal data held about the requester with third parties.[21]

The banking sector has been the first sector designated sector to commence roll-out of the CDR through the concept of 'open banking'. The banking sector has made considerable progress, turning to the contractual agreements with the fintechs themselves to ensure progress of the implementation of the CDR is not stifled in the interim.

Redress and enforcement

Individuals do not have a direct cause of action against offending agencies in respect of infringement of the Privacy Act (including the IPPs). However, an aggrieved individual or group of individuals may complain to the Commissioner who may hear the complaint and determine an appropriate course of action to secure settlement of the complaint.

In certain circumstances if a complaint has been made to the Commissioner, aggrieved individuals may file a claim with the Tribunal.[22] If successful, the Tribunal may award compensatory damages for losses suffered.

iv Specific regulatory areas

While the Privacy Act applies to the processing of personal information generally, codes of practice issued under the Act may modify the application of the IPPs and set privacy rules relevant to specific classes of information, industry sectors or classes of agency subject to the Act.

20 Privacy Act, Part 4.

21 Ministry of Business, Innovation and Employment (MBIE), 'Customer and Product Data Bill'.

22 Privacy Act, Section 98.

As at the time of writing, six codes of practice have been issued under the Act, modifying the IPPs and privacy rules as applicable to specific sectors including healthcare, telecommunication and credit reporting. An additional code of practice is likely to be developed in the near term, modifying the IPPs and privacy rules as applicable to biometric technologies.

While surveillance is generally regulated under the Privacy Act, state-based surveillance is separately regulated under the Intelligence and Security Act 2017 and the Search and Surveillance Act 2012.

Electronic marketing is regulated by the Unsolicited Electronic Messages Act 2007.

The Digital Identity Services Trust Framework Act 2023 was passed this year to streamline and regulate the use of digital identities in New Zealand. As a 'standalone' piece of legislation, digital identity service providers are able to opt-in to compliance under this legal framework for recognised accreditation.[23]

v Technological innovation

The Privacy Act is technologically neutral, adopting a principle-based approach to minimise the need for substantial reform to account for technological change. This technology neutral and principle-based framework was retained following the substantive reform of New Zealand's privacy legislation in 2020.

Biometric technologies

One area of technological innovation that has received recent consideration from the OPC has been biometrics and facial recognition technologies. In October 2021, the OPC released a detailed position paper on how the Privacy Act regulates biometrics confirming the OPC's view that the IPPs and the existing tools in the Privacy Act are sufficient to regulate the use of biometrics from a privacy perspective. In August 2022, the OPC published a subsequent consultation paper on privacy regulation of biometrics in New Zealand and sought submissions in response to that paper. The OPC has indicated that its initial position paper on how the Privacy Act regulates biometrics will likely be reconsidered, reflecting a strong call to action for express privacy regulation of biometrics in New Zealand. This is likely to be in the form of a specific code of practice (discussed further at Section III.iv).

Generative artificial intelligence

In New Zealand, widespread adoption of generative AI tools such as OpenAI's ChatGPT has triggered the OPC to release guidance setting out the OPC's expectations regarding the use of generative AI. The Commissioner has emphasised that given that New Zealand's Privacy Act is technology-neutral, the Act will apply to the use of generative AI technologies, and agencies considering whether to use a generative AI tool need to be aware of potential privacy risks that have been associated with these tools,[24] including the following.

23 DIGITAL.GOVT.NZ, 'Key Concepts of the Trust Framework' (18 January 2022).

24 https://www.privacy.org.nz/publications/guidance-resources/generative-artificial-intelligence-15-june-2023-update/.

Source and legality of training data used by the generative AI

As generative AI models are trained on large quantums of information (including personal information), privacy risks are inherent in the use of that training data. Businesses need to appropriately understand how the relevant personal information has been collected, whether that information is accurate and whether that information can in fact be used for the purposes of the generative AI tool.

Confidentiality of input data

Prompts used in connection with generative AI tools could include personal and confidential business information. Businesses would need to ensure they have the appropriate authorisations to use the personal or confidential information for the purpose of these prompts. To the extent that the provider of the generative AI tool continues to use that prompt data for training of the model, further consents may need to be obtained.

Individual rights of access and correction to personal information

Generative AI tools may not always be compatible with the rights of access and correction to personal information provided for under the Privacy Act.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

New Zealand privacy law provides that personal information may only be disclosed to foreign entities or persons[25] in prescribed circumstances.[26] These prescribed circumstances include:

a where the individual concerned authorises the disclosure after being expressly informed that the foreign recipient may not be required to protect their information in a way that provides comparable safeguards to those under New Zealand law;

b where the foreign recipient is carrying on business in New Zealand; or

c the disclosing agency believes on reasonable grounds that the foreign recipient is:

- subject to privacy laws that provide comparable safeguards to those under New Zealand privacy law; or
- required to protect the information in a way that provides comparable safeguards to those under New Zealand privacy law (for example, pursuant to an agreement between the disclosing agency and the foreign entity).[27]

Accordingly, if the jurisdiction in which the foreign entity is located does not offer comparable protections to those under the Privacy Act (and appropriate contract terms providing for such comparable safeguards cannot be put in place), the individual concerned must be fully informed that their information may not be adequately protected and they must expressly authorise the relevant disclosure.

25 Foreign entities and persons including foreign governments, individuals not ordinarily resident in New Zealand and businesses and organisations not established under New Zealand laws or with central management in New Zealand.

26 Privacy Act, Section 22 (IPP12).

27 The OPC has developed model contractual clauses for this purpose. These model clauses reflect the Schrems II decision regarding the EU–US Privacy Shield where the validity of standard contractual clauses was upheld, but it requires companies and regulators to conduct case-by-case analysis to determine whether foreign protections concerning government access to data transferred meet the EU standards.

Disclosures of personal information to offshore cloud providers or other agents to store or process data on behalf of the disclosing agency are not treated as 'disclosures of personal information' under the Privacy Act, so long as the agent or cloud provider does not use the information for their own purposes.[28] As information transferred out of New Zealand for storage and processing purposes is still considered to be held by the transferring agency, the transferring agency will continue to be bound by many of the IPPs in respect of that information transferred outside of New Zealand.

The Commissioner may prohibit a transfer of personal information from New Zealand to another country if the Commissioner is satisfied, on reasonable grounds, that:

a the information has been, or will be, received in New Zealand from another country and is likely to be transferred to a third country where it will not be subject to a law providing comparable safeguards to those under the Privacy Act; and

b the transfer would be likely to lead to a contravention of the basic principles of national application set out in Part Two of the OECD Guidelines.[29]

This power will not apply where the transfer of data is required by New Zealand law or any convention or other instrument imposing international obligations on New Zealand.

Under New Zealand privacy law, there are no mandatory requirements to store prescribed classes or sets of personal information exclusively within New Zealand. However, there are limited sector-specific laws that imply a data localisation requirement for certain categories of non-personal data. For example, under the Goods and Services Tax Act 1985, GST-registered persons are required to keep and retain prescribed records at a place in New Zealand unless otherwise authorised by the Commissioner of Inland Revenue.

V COMPANY POLICIES AND PRACTICES

The Privacy Act does not generally mandate prescriptive policies and practices for adoption by agencies subject to the Act. However, there are a number of key legislative requirements and best practice guidelines that are worth noting:

i Privacy statements

Where personal information is collected directly from an individual, the collecting agency must take reasonable steps to ensure that the individual is aware of certain prescribed matters (discussed in Section III.iii) before the information is collected or as soon as practicable after the information is collected.[30] Online privacy statements together with internal privacy policies are generally used to inform individuals of these prescribed matters.

28 Privacy Act, Section 11.

29 id., Section 193.

30 id., Section 22 (IPP3).

ii Privacy officers

Agencies are required to appoint one or more individuals as privacy officers.[31] The responsibilities of a privacy officer include:

a encouraging the agency to comply with the IPPs and ensuring that the agency complies with the Act;

b dealing with requests made to the agency under the Act; and

c working with the Commissioner in relation to investigations in respect of the agency's conduct with respect to the Act.

iii Best practice

While not mandated by New Zealand privacy law, it has also been generally accepted that businesses should undertake the following to help ensure compliance with the IPPs:

a conduct data mapping exercises to understand the data sets collected by the business and how those data sets are collected, used, stored, shared and otherwise processed;

b conduct regular internal privacy compliance training;

c maintain internal privacy and data management policies including:
- data breach response plans;
- data retention and destruction policies;
- AI policies (where applicable);
- data security and disaster recovery policies; and
- governance polices covering escalation of privacy-related requests and incidents;

d ensure issues related to privacy compliance and data management are prioritised within management and at the board level;

e application of the concept of 'data minimisation' when collecting personal information;[32]

f ensure privacy impact assessments are undertaken for new or revised information handling or sharing practices; and

g encouragement of a 'privacy by design' approach to development of new products and business tools.

There also exists sector-specific guidance on the role of governance in cybersecurity from New Zealand regulators (see Section IX).

iv Guidelines for generative AI

In June 2023, the OPC released guidance with respect to the use of generative AI technologies by agencies subject to the Privacy Act.[33] The guidance issued will continually be adapted as AI technologies continue to evolve and the OPC continues to reassess its approach.[34] The OPC's expectation is that agencies subject to the Privacy Act will take the following actions[35] when implementing a generative AI tool:

a obtain explicit senior leadership approval after full consideration of the risks and necessary mitigations to be actioned before adopting the generative AI tool;

31 id., Section 201.

32 Privacy Commissioner, 'New Zealand's biggest data breach shows retention is the sleeping giant of data security' (3 April 2023).

33 Privacy Commissioner, 'Generative Artificial Intelligence – 15 June 2023 update'.

34 id.

35 id.

b in light of the potential privacy implications, review whether it is necessary and proportionate to use a generative AI tool in the first instance;

c conduct a privacy impact assessment (or algorithmic assessment, or both) to highlight any privacy risks before implementation;

d be transparent about how, when and why the generative AI tool is being used and how potential privacy risks are being addressed;

e engage with Māori stakeholders;

f develop internal procedures to ensure that where personal information is collected through a generative AI tool the personal information is accurate and that where necessary, the agency is able to provide access to this information where requested;

g maintain human oversight; and

h where possible, ensure that personal or confidential information is not retained or disclosed by the generative AI tool.

VI DISCOVERY AND DISCLOSURE

Under New Zealand privacy law, personal information can generally only be disclosed for the purposes in connection with which it was originally obtained (or a directly related purpose) unless the disclosing agency believes, on reasonable grounds, that a prescribed exception applies.

Disclosure of personal information in response to national or foreign government requests, or in response to domestic or foreign civil discovery court orders or internal investigations is not expressly permitted by New Zealand privacy law; however, as mentioned above there are a number of prescribed exceptions to the general rule against disclosure that may apply.

In legal proceedings, disclosure of personal information is permitted if the disclosure of the information is necessary for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation).[36]

Further, in respect of disclosures to government agencies or in respect to court orders, disclosure is permitted where:

a the disclosure of that information is otherwise authorised by another New Zealand law (which would allow disclosures that are required or authorised by court rules); or

b the disclosure is necessary:

- to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution and punishment of offences;
- for the enforcement of a law that imposes a pecuniary penalty; or
- for the protection of public revenue.

With respect to disclosures outside of New Zealand, an action taken by an agency in relation to information held overseas does not breach the general rule against disclosure if the action is required by or under the law of any country other than New Zealand.[37] While this exception

36 id., Section 22 (IPP11).

37 id., Section 23.

may assist disclosures of information held overseas where disclosure is required under the laws of that jurisdiction, this exception does not apply in respect of information held within New Zealand.

In respect of disclosures required for the purposes of national security or serious crime surveillance in New Zealand, disclosure is permitted where it is necessary:

a to prevent or lessen a serious threat to public health or public safety or the life or health of the individual concerned or another individual; or

b to enable the New Zealand Security Intelligence Service or Government Communications Security Bureau to perform any of its functions.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The OPC is the regulator responsible for investigating compliance with and enforcing the Privacy Act.

The Privacy Act gives the Commissioner power to investigate privacy complaints. Such investigations are exercised by the Commissioner through the OPC. The role of the OPC in respect of any privacy complaint is to determine if there has been a breach of the Privacy Act and to facilitate a resolution between the parties. The OPC does not have the power to force organisations to pay damages or force aggrieved parties to accept a settlement offer.

The OPC may also commence investigations on its own initiative, into any matter in respect of which a complaint may be made under the Privacy Act.[38]

The OPC may refer a privacy complaint to the Director of Human Rights Proceedings (the Director) who may decide whether to commence proceedings in the Tribunal in respect of the complaint.

If the Tribunal is satisfied that there has been a privacy infringement, the Tribunal may grant a number of remedies including declarations, restraining orders, awarding damages or issuing orders for specific performance.

The OPC also has the power to issue a compliance notice to organisations and businesses that are not meeting their obligations under the Privacy Act.[39] These notices may require the organisation or business to do something, or to stop doing something, to comply with the Privacy Act. The OPC may publish details of a compliance notice if the Commissioner believes it is desirable to do so in the public interest.[40]

ii Recent enforcement cases

The Commissioner's Annual Report 2022[41] recorded that during the year ending 30 June 2021, the OPC:

a received 486 privacy complaints for review;[42]

b received 657 privacy breach notifications;[43] and

38 id., Section 79(b).

39 id., Section 123(1).

40 id., Section 129.

41 Privacy Commissioner, 'Annual Report 2022' (30 June 2022).

42 id., 6.

43 id.

c noted that of the privacy complaints closed, 40 per cent were closed by settlement between the parties.[44]

In September 2022, the OPC announced the closure of its first (and to date only) compliance notice issued under the Privacy Act.[45] The compliance notice, issued to RBNZ in September 2021, was triggered by a cyberattack in December 2020 (discussed further in Section IX).

Some notable recent enforcement actions include:

a in May 2023, the OPC and the Office of the Australian Information Commissioner (OAIC) commenced a joint investigation into a data breach impacting Latitude Financial. This is the first joint privacy investigation by Australia and New Zealand, which followed preliminary inquiries into the matter by both offices. The investigation is currently ongoing and is focused on whether Latitude took reasonable steps to protect the personal information it held from misuse, interference, loss, unauthorised access, modification or disclosure as well as whether Latitude took appropriate steps to destroy or de-identify personal information that was no longer required;[46]

b in March 2022, the Tribunal awarded damages totalling NZ$100,000 against Netsafe Inc after finding that the actions of Netsafe in its refusals of three personal information access requests were interferences with the privacy of the three individuals;[47]

c in late 2021, the Commissioner intervened in judicial review proceedings in relation to the disclosure of Māori vaccination information.[48] This proceeding was concerned with the use of Māori data by the Ministry of Health and the interpretation of the serious threat to public health exception in Rule 11(2)(d) of the Health Information Privacy Code during the covid-19 pandemic; and

d in March 2015, the Tribunal awarded damages totalling approximately NZ$168,000 against Credit Union Baywide (being the largest sum of damages to date in respect of a privacy related claim).[49] Credit Union Baywide compelled an employee to access a former employee's Facebook page, in breach of that former employee's privacy settings, to access and maliciously distribute a photo of a cake prepared by the former employee featuring derogatory language directed at Credit Union Baywide to third parties (including that former employee's new employer).

iii Private litigation

Under New Zealand privacy law, individuals do not need to use the courts to enforce their rights. Instead, as discussed in Sections VII.i and VII.ii, individuals generally bring complaints to the Commissioner for resolution. Nonetheless private litigation can be brought before the courts. For example, Privacy Act cases that are not resolved through the Commissioner's processes can be taken to the Tribunal (which is part of New Zealand's system of specialist

44 id., 38.

45 Privacy Commissioner, 'First Privacy Act compliance notice successfully closed' (1 September 2022).

46 https://privacy.org.nz/publications/statements-media-releases/new-zealand-australia-investigation-into-latitude-breach-begins/.

47 *Director of Human Rights Proceedings v. Netsafe Inc* [2022] NZHRRT 15.

48 *Te Pou Matakana Limited v. Attorney-General (No. 1)* [2021] NZHC 2942; and *Te Pou Matakana Limited v. Attorney-General (No. 2)* [2021] NZHC 3319.

49 *Hammond v. Credit Union Baywide* [2015] NZHRRT 6.

statutory tribunals). Cases can be appealed from the tribunal through the New Zealand court system. Private parties may also use judicial review to challenge a public sector agency's decision with respect to personal information.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

i Extraterritorial application of the Privacy Act

The Privacy Act applies to actions undertaken by overseas agencies in the course of carrying on business in New Zealand in respect of personal information collected or held by that agency, regardless of where the information was collected or held and where the person to whom the information relates is located.[50]

The Act does not expressly prescribe what it means to 'carry on business in New Zealand'; however, it does provide that an agency may be considered to be carrying on business in New Zealand irrespective of whether the agency:

a has a place of business in New Zealand;
b is a commercial operation or receives any money for the supply of goods and services; or
c intends to make a profit from its business in New Zealand.[51]

The Act's extraterritorial effect will, however, not extend to the government of an overseas country, an overseas government entity to the extent that the entity is performing any public function on behalf of the overseas government or a news entity, to the extent that it is carrying on news activities.[52]

ii Localisation requirements

Under the Privacy Act, there are no mandatory localisation requirements to store any class or category of personal information exclusively within New Zealand. However, as discussed in Section IV, there are limited sector-specific laws that imply a data localisation requirement for certain categories of non-personal data. For example, under the Goods and Services Tax Act 1985, GST-registered persons are required to keep and retain prescribed records at a place in New Zealand unless otherwise authorised by the Commissioner of Inland Revenue.

Further, as discussed in Sections IV and IX, agencies subject to the Privacy Act are subject to:

a IPP12, which requires businesses and organisations to ensure that personal information transferred overseas is adequately protected; and
b IPP5, which requires businesses and organisations that hold personal information to ensure that the information is protected by reasonable security safeguards against loss or unauthorised access, use, modification or disclosure.

Compliance with the above IPPs may naturally pose challenges of transfers to personal information to certain jurisdictions.

50 Privacy Act 2020, Section 4.
51 id., Section 4(3).
52 id., Section 9.

IX CYBERSECURITY AND DATA BREACHES

i Privacy Act – cybersecurity

Under the Privacy Act, IPP5 requires all agencies that hold personal information to ensure that the information is protected by reasonable security safeguards against loss or unauthorised access, use, modification or disclosure.[53]

The Privacy Act does not prescribe any specific security standards to ensure compliance with IPP5. What safeguards are reasonable for an agency to take will depend principally on the circumstances, including factors such as:

a how sensitive is the personal information involved and what is the relevant agency using the personal information for;

b what security measures are available; and

c what the consequences might be should the information not be kept secure.

Privacy impact assessments (discussed in Section V) are encouraged as a matter of best practice to help businesses identify and appropriately manage potential cybersecurity risks from a privacy perspective practically prior to introduction or adoption of a new cybersecurity policy.

The Commissioner may issue compliance notices to organisations that are not meeting their obligations under the Privacy Act, including compliance with IPP5. In September 2021 the Commissioner issued its first compliance notice to RBNZ to make their systems more secure for handling personal information and take certain steps within prescribed time frames to comply with IPP5. The compliance notice was triggered following a cyberattack affecting the organisation which exploited a weakness in one of RBNZ's third-party systems. The compliance notice was formally closed on 1 September 2022.[54]

ii Privacy Act – mandatory privacy breach notification

There are no general mandatory reporting requirements specifically for cyber incidents in New Zealand; however, the Privacy Act requires organisations to notify the Commissioner as well as affected individuals in the event of a 'notifiable privacy breach'. A notifiable privacy breach occurs where:

a there is unauthorised or accidental access to or authorised disclosure, alternation, loss or destruction of someone's personal information or someone is unable to access their personal information (either on a temporary or permanent basis); and

b it is reasonable to believe that the breach has caused serious harm to an affected individual or individuals or is likely to do so.[55]

In the year ending 30 June 2022, the OPC reported that it had received 657 notifications (being a slight decrease on the year prior). Approximately 85 per cent of all reported privacy breaches occurred within the healthcare and social assurance industries.[56]

53 id., Section 22, IPP5.

54 Privacy Commissioner, 'First Privacy Act compliance notice successfully closed' (1 September 2022).

55 id., Section 112.

56 Privacy Commissioner, 'Privacy Commissioner Annual Report 2022 (June 30 2022), 10.

iii Government Communications Security Bureau (GCSB), the National Cyber Security Centre (NCSC) and New Zealand's Computer Emergency Response Team (CERT NZ)

The GCSB provides advice, assistance and protective security services to public authorities and other persons authorised to receive support from the Bureau. The NCSC is part of the GCSB and responds to threats to nationally significant organisations and high-impact cyber incidents at a national level. In the NCSC's annual cyber threat report for the 2021/ 22 year, the NCSC recorded 350 incidents with a possible national impact or affecting New Zealand's nationally significant organisations (considered by the organisation to reflect a small but impactful portion of all cybersecurity incidents affecting New Zealand).[57] An important trend reflected in the relevant incidents is the prominence of criminally motivated activity – 23 per cent of NCSC's recorded incidents for the 2021/22 year showed indicators of suspected criminal or financially motivated actors (down 4 per cent on the prior year).[58]

NCSC works closely with organisations like CERT NZ. CERT NZ supports businesses, organisations and individuals who are affected (or may be affected) by cybersecurity incidents including by triaging reported incidents and coordinating an organisation's response to a reported incident.

iv Cybersecurity and the role of other regulators

Financial Markets Authority

The Financial Markets Authority (FMA) has been active in promoting the cyber-resilience of the entities it supervises (which, as New Zealand's securities regulator, include a broad range of financial market participants). Following a thematic review, the FMA published a report in July 2019[59] that provided a number of recommendations for the management of cyber risk by regulated entities, including:

a using services provided by CERT NZ and the NCSC;
b using a recognised cybersecurity framework to assist with planning, prioritising and managing cyber resilience;
c having an appropriate balance between protection and detection measures; and
d board or senior management ownership and visibility of the cyber resilience framework.

In July 2023, the FMA released a consultation documentation on the proposed new standard condition for certain financial market license holders aiming to promote cyber resilience.[60] The new standard condition will require these licence holders to have a business continuity plan in place to ensure that their IT systems are 'operationally resilient'.[61]

57 National Cyber Security Centre, 'Cyber Threat Report 2021/22', 2.
58 id.,2.
59 Financial Markets Authority, 'Cyber-resilience in FMA-regulated financial services' (July 2019).
60 Financial Markets Authority, 'Consultation: Proposed standard condition on business continuity and technology systems' (July 2023).
61 id., 3.

Reserve Bank

In April 2021, RBNZ published guidance for RBNZ-regulated entities (including registered banks, licensed non-bank deposit takers and licensed insurers) to set RBNZ's expectations for those entities in respect of cyber resilience.[62] RBNZ's guidance is intended to serve as an overarching framework for the governance and management of cyber risk for RBNZ-regulated entities as opposed to a prescribed set of rules with which those entities must comply – the emphasis being on the role of governance within the sector in appropriately managing cyber risks.

X SOFTWARE DEVELOPMENT AND VULNERABILITIES

In New Zealand there are no legislative instruments specifically dedicated to regulating software development or the management of software vulnerabilities. However, in addition to intellectual property and consumer laws, there are a number of key legal requirements that both software developers and customers procuring software solutions must have regard to.

i Privacy Act

As discussed in Section IX.i, under the Privacy Act, IPP5 requires agencies that hold personal information to ensure that the information is protected by reasonable security safeguards. While specific security standards are not prescribed by the Privacy Act, IPP5 places the onus on organisations and businesses holding personal information to ensure that any software used to store or otherwise process that information enables compliance with IPP5.[63]

To the extent a 'notifiable privacy breach' (discussed in Section IX.ii) occurs as a result of a software defect or exploitation of a software vulnerability, the organisation suffering the breach will be required to report the incident to the Privacy Commissioner and affected individuals.[64]

ii Generative AI

To the extent software incorporates or derived from generative AI, developers and users subject to the Privacy Act should bear in the Privacy Commissioner's guidance in relation to the use of generative AI technologies (discussed further in Section V.v).[65]

iii Government Protective Security Requirements

The development and use of software by government agencies is subject to additional regulation. The Protective Security Requirements (PSR) is the New Zealand government's best practice security policy framework.[66] The PSR outlines the government's expectations for security governance and for personnel, information and physical security and sets out 20 mandatory requirements with which certain government agencies must comply. Compliance with the PSR is mandatory for certain government agencies, and private sector compliance is

62 Reserve Bank of New Zealand, 'Guidance on Cyber Resilience' (April 2021).

63 Privacy Act, Section 22, IPP5.

64 Privacy Act, Section 117.

65 Privacy Commissioner, 'Generative Artificial Intelligence – 15 June 2023 update'.

66 https://protectivesecurity.govt.nz/about-the-psr/.

also encouraged. The New Zealand Information Security Manual (NZISM)[67] is an integral part of the PSR framework and details processes and controls essential for the protection of all New Zealand government information and systems, including specific controls applicable to software application development.

XI DIGITAL GOVERNANCE AND CONVERGENCE WITH COMPETITION POLICY

i Data privacy and competition policy

The Commerce Act 1986 remains New Zealand's primary legislative tool for regulating anticompetitive practices across markets in New Zealand (including digital markets and the technology sector). Echoing the sentiment of regulators around the world, New Zealand regulators are actively considering whether New Zealand's existing competition laws are sufficiently robust to operate in the era of big tech, a common theme of such commentary being that specific regulation of digital markets from a competition standpoint (i.e., data portability, additional notification) is required.

In March 2022, New Zealand's Ministry of Business, Innovation and Employment (MBIE), produced a final report on behalf of the Asia Pacific Economic Cooperation (APEC) Competition Policy and Law Group covering the relationship between competition law, consumer protection and data protection in the context of the digital economy and options to facilitate better cross-border cooperation between competition and regulatory agencies.[68] The report highlighted concerns about New Zealand's lack of regulatory settings, which at that time were viewed as hindering consumer data portability in New Zealand.[69] As discussed in Section II.ii, in June 2023, MBIE opened consultation on the CDR Bill. The Bill will create a statutory right for consumers to require entities holding their personal information to share that information with accredited third party services. The intent behind the CDR Bill is to ultimately increase competition, enhance business efficiency and help customers access and compare products that will better meet their needs.

ii Digital content regulation

New Zealand's Department of Internal Affairs (DIA) is currently seeking public feedback on a discussion document addressing digital content regulation.[70] The overarching proposal is to have one regime that regulates all forms of platform across all types of digital content, New Zealand currently having multiple regulators in the media content sector, including multiple regulators for online content. The livestreaming of the Christchurch terror attack video in March 2019 was a stark demonstration of the failings of New Zealand's current content regulations, such regulations being designed around traditional ideas of content, books, magazines and free-to-air TV and largely no longer fit for purpose in the context of the evolving digital environment.

67 https://www.nzism.gcsb.govt.nz/ism-document/.

68 Ministry of Business, Innovation and Employment for the APEC Competition Policy and Law Group, 'Competition Law and Regulation in Digital Markets FINAL REPORT' (March 2022).

69 id., Appendix II. APEC Economy Survey Responses.

70 Department of Internal Affairs, 'Safer Online Services and Media Platforms – Discussion Document' (June 2023).

XII OUTLOOK

Notwithstanding that New Zealand privacy law has recently undergone significant reform with the introduction of the new Privacy Act 2020, there continues to be ongoing debate as to whether the new Act went far enough and whether the enhanced privacy protections are sufficient to warrant the retention of New Zealand's adequacy status with the EC, currently under review.

A close watching brief will be kept on the EC's review of New Zealand's adequacy status. If New Zealand's status is revoked, then the administrative requirements are more onerous for transfers of personal data between New Zealand and the EU (and now also the UK); for example, organisations and business that share between the EU and New Zealand may be required to enter into a data transfer agreement based on the EC's Standard Contractual Clauses.

Further, as malicious cyberactivity in New Zealand continues to rise, we are curious as to whether more prescriptive cyber legislation for New Zealand is tabled in the near future (particularly given the substantive reform for cybersecurity regulation recently undertaken in Australia).

ISBN 978-1-80449-214-7