Protecting Māori data: Can a Privacy Code of Practice provide a partial solution?

David Watts & Tahu Kukutai

Tikanga in Technology Discussion Paper

November 2025

Te Ngira Institute for Population Research
THE UNIVERSITY OF WAIKATO

Tikanga in Technology

To cite this publication

Watts, D. & Kukutai, T. (2025). *Protecting Māori data: Can a Privacy Code of Practice provide a partial solution?* Tikanga in Technology discussion paper. Hamilton: Te Ngira Institute for Population Research. 10.15663/f42.19700

This report was funded by a Ministry of Business, Innovation and Employment (MBIE) Endeavour Grant (UOWX2003) for the research programme *Tikanga in Technology: Transforming Māori and Indigenous data ecosystems*.

Acknowledgements

We thank reviewers for their comments on earlier drafts of this paper including Jesse Porter, Lynell Tuffery Huria and Ella Pēpi Tarapa-Dewes. Any errors or omissions are ours alone.

Definitions

Māori data

Māori data refers broadly to digital or digitisable data, information or knowledge (including mātauranga Māori) that is about, from or connected to Māori. It includes data about population, place, culture and environment.

Māori data governance

The principles, structures, accountability mechanisms, legal instruments and policies through which Māori exercise control over Māori data.

Māori data sovereignty

The inherent rights and interests that Māori have in relation to the collection, ownership and application of Māori data.

Glossary

Aotearoa	New Zealand
hapū	subtribe, clan
hui	meeting
iwi	tribe
kaitiaki	guardian
kawa	immutable protocols
mana	spiritual authority, power, influence, status, prestige
marae	customary Māori gathering space, typically comprising buildings and a courtyard area
marae ātea	the open area in front of the wharenui (meeting house) where formal welcomes to visitors takes place and issues are debated
mātauranga Māori	Māori knowledge systems and ways of knowing
mauri	life force
noa	unrestricted, be free of tapu, to make common
rangatahi	Māori youth
taonga	those things and values that we treasure, both intangible and tangible
tapu	sacred, restricted or prohibited
te ao Māori	the Māori world
te Tiriti o Waitangi	the Treaty of Waitangi
tika	correct, appropriate, right
tikanga	values and practices for proper conduct
tohunga	high priest; an expert of their field of knowledge
whakanoa	to remove tapu
whakapapa	genealogy; lineage
whānau	family

Initialisms

AI	artificial intelligence
DNA	deoxyribose nucleic acid; that is, genetic material
ESR	The Institute of Environmental Science and Research (rebranded as New Zealand Institute for Public Health and Forensic Science (PHF Science) as of 1 July 2025).
FGG	forensic genetic genealogy
FIGG	forensic investigative genetic genealogy
FPIC	free, prior and informed consent
FRT	facial recognition technology
GDPR	General Data Protection Regulation
ICCPR	International Covenant on Civil and Political Rights
IDSov	Indigenous data sovereignty
IPPs	(the) Information Privacy Principles (of the Privacy Act 2020)
MBIE	Ministry of Business, Innovation and Employment
MDP	Māori data privacy
MDSov	Māori data sovereignty
OECD	Organisation for Economic Co-operation and Development
OPC	Office of the Privacy Commissioner
OT	Oranga Tamariki
SNP	single nucleotide polymorphism; a very short extract of DNA
TiNT	Tikanga in Technology research programme
TMR	Te Mana Raraunga
UDHR	Universal Declaration of Human Rights
UNDRIP	United Nations Declaration on the Rights of Indigenous Peoples
UNESCO	United Nations Educational, Scientific and Cultural Organization

Abstract

This paper explores whether a Māori Data Privacy (MDP) Code, developed under the Privacy Act 2020 (the Act), could provide additional protection for classes of information that are regarded by Māori as tapu. The Act already covers the personal information of Māori individuals in the same way it does any other individual. We argue that a MDP Code could offer additional protection for classes of sensitive personal information – specifically whakapapa data and data pertaining to deceased Māori. A MDP Code could restrict the purposes for which such information can be collected, used, disclosed, retained, stored and disposed of; put stronger requirements on agencies to demonstrate that their collection and use of this information is justified; require free, prior and informed consent for its use and disclosure; and provide for greater transparency and independent Māori oversight.

Table of Contents

PART 1. INTRODUCTION

Purpose

This paper is part of a series, undertaken for the *Tikanga in Technology* (TiNT) research programme, that examines Māori approaches to information privacy. Its main purpose is to explore whether a Māori Data Code, developed under Aotearoa New Zealand's Privacy Act 2020 (the Act), could provide additional protection for classes of Māori data that are regarded as tapu.[1] Our primary intent is to provide a research-informed analysis that assists legislators, regulators and policy makers in Aotearoa NZ to better understand, recognise and give effect to Māori privacy perspectives through existing legal and regulatory frameworks.

Although our focus is on Aotearoa NZ, the methodology we have adopted can be replicated by other Indigenous peoples who wish to explore the extent to which their culturally sensitive information might be protected under data protection law.[2] Most worldwide data protection laws (including the Act) are based on the Organisation for Economic Cooperation and Development's (OECD) *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*[3] (OECD Guidelines). These are implemented differently jurisdiction by jurisdiction and have been augmented by some additional rights.[4] Our approach provides an overall roadmap that can assist Indigenous peoples to explore the intersection between rights to privacy (or akin to privacy) under traditional law and custom, and under data protection laws that have been informed by the OECD guidelines.

Background and context

In Aotearoa NZ, privacy is protected through common law and under the Act. The Act focuses on one important dimension of privacy: information privacy. In broad terms, it provides individuals with a measure of control over the way in which their personal information is collected and handled in both the public and private sectors. Its purposes are

[1] A glossary of Māori terms is provided at the front of this paper.
[2] In this paper we use the terms 'data protection' and 'information privacy' synonymously.
[3] Organisation for Economic Cooperation and Development (2013). *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (adopted 1980, amended 2013). https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188
[4] For example in the *General Data Protection Regulation,* A 17 (the 'right to be forgotten') and A 21 (the right to object and automated individual decision-making).

"to promote and protect individual privacy by providing a framework for protecting personal information" and by "giving effect to international privacy obligations and standards".[5, 6] The centrepiece of the Act's information privacy protections is the *Information Privacy Principles* (IPPs). These regulate the way in which agencies collect, use, disclose, secure and otherwise handle personal information as well as provide individuals with rights to access and correct their personal information. Personal information is defined as "information about an identifiable individual",[7] and includes information relating to a death that is maintained by the Registrar-General.[8]

In a previous TiNT paper on Māori data sovereignty (MDSov) and privacy, we argued that the Act does not adequately protect Māori data, due to its lack of statutory recognition of collective dimensions of privacy, te Tiriti o Waitangi and tikanga Māori (tikanga) (Kukutai, Cassim, et al., 2023). However, the Act includes powers that enable the Privacy Commissioner (the Commissioner) to adapt and tailor the IPPs to address particular categories of privacy risks. These are the Commissioner's powers to issue a code of practice (Codes) under Part 3, Subpart 2 of the Act. This paper explores the extent to which these code-making powers may be used to better protect Māori data, particularly data that are culturally sensitive. This requires more than a narrow analysis of the Commissioner's code-making powers – a more comprehensive and nuanced approach is necessary. The reason for this approach is that the code provisions, particularly s 32 and s 33 of the Act, are informed and shaped by requirements that the Commissioner must regard in making discretionary decisions about the development, scope and content of a code. These include:

- cultural perspectives about privacy (s 21(c)),
- international obligations accepted by Aotearoa NZ (s 21(b)), and
- the privacy rights of individuals alongside other human rights and interests (s 21(a)).

For Māori, cultural perspectives about privacy are grounded in tikanga, often defined as Māori customary values and practices, and more formally as a normatively proper way of being, acting and conducting affairs in the community, informed by common cultural values and concepts (Benton et al., 2013; Mead, 2013). In its comprehensive review of the now-repealed Privacy Act 1993, the Law Commission stressed the importance of understanding

[5] See Privacy Act 2020, s 3(b).
[6] Section 3(a).
[7] Section 7(1).
[8] Section 7(1).

tikanga approaches to privacy and recommended that the Act be amended to require the Commissioner to take account of Māori needs and cultural perspectives (Law Commission, 2011, p. 33). The Office of the Privacy Commissioner (OPC) has publicly stated its willingness to consider how the IPPs might be modified specifically in relation to Māori data (Office of the Privacy Commissioner, 2023a, p. 8) and has assembled a Māori Reference Panel to provide Māori expertise and input to its work.[9] However, since the current Act came into force in 2020, there have been few examples of the Commissioner taking account of tikanga perspectives about information privacy in exercising their powers and carrying out their functions and duties (Kukutai, Cassim et al., 2023; Quince & Houghton, 2023). One exception is the guidance on "Cultural impacts and effects on Māori" for the Biometric Processing Privacy Code which came into force on 3 November 2025 (Office of the Privacy Commissioner, 2025a, 2025b).[10] The guidance recognises the importance of tikanga and Māori data sovereignty in relation to biometric processing but is non-binding and thus not legally enforceable.

Structure of this paper

The structure of this paper is as follows. First, we provide a brief account of how tikanga served to regulate individual and collective conduct, including in relation to the protection and disclosure of restricted knowledge, and to identify key elements of Māori understandings of privacy. Second, we turn to the concept of privacy and discuss what it entails, including the categories of privacy protections currently recognised under Aotearoa NZ law. Finally, we consider the Commissioner's discretionary code-making powers and examine how they can be used to provide additional protection for Māori data, focusing on specific classes of sensitive Māori data: whakapapa data and data about deceased Māori.

[9] One of this paper's authors, Tahu Kukutai, is a member of the Panel.

[10] The Code requires organisations to assess the cultural impacts and effects of biometric processing on Māori (Rule 1, s 3(c) but does not refer specifically to tikanga. We note that OPC has referred to the importance of tikanga and Māori perspectives on privacy in other contexts. The Joint inquiry by the Independent Police Conduct Authority and the Privacy Commissioner into Police conduct when photographing members of the public (OPC & IPCA, 2022) has a brief section on tikanga considerations (pp. 104-105), although they are absent in the report's 23 recommendations. OPC's inquiry into Foodstuffs North Island use of facial recognition technology (OPC, 2025c) noted concerns raised by Māori stakeholders including tikanga considerations (p. 22-23). The Privacy Commissioner's interventions in the Te Pou Matakana cases (No 1, 2021; No 2, 2021) did not refer to tikanga directly but did note s 21c of the Act requiring consideration of cultural perspectives: https://www.privacy.org.nz/resources-and-learning/court-decisions/case-note-high-court-decisions-te-pou-matakana-limited-v-attorney-general-no-1-2021-nzhc-2942-and-no-2-2021-nzhc-3319/

PART 2. TIKANGA AND ITS RELEVANCE FOR DATA PRIVACY

There is a significant body of scholarship that discusses the relevance and implications of tikanga for the Aotearoa NZ legal system, which can serve as a basis for understanding how these normative rules and practices apply to Māori data privacy. Examples include:

- the 2001 Law Commission study paper 9, *Māori custom and values in New Zealand,* examining the intersection between tikanga and state law
- the 2023 Law Commission study paper 24, *He Poutama,* updating the 2001 study and further examining the place of tikanga in the Aotearoa NZ legal landscape
- Moana's Jackson's 2000 paper on sovereignty in *Building the Constitution*
- Ani Mikaere's 2007 article on tikanga as the first law of Aotearoa NZ in the *Yearbook of New Zealand Jurisprudence*, and
- Natalie Coates's 2017 paper on the recognition of tikanga in Aotearoa NZ common law.

A number of statutes recognise and give effect to tikanga, including the Resource Management Act 1991, the Oranga Tamariki Act 1989, the Education and Training Act 2020, and the Employment Relations Act 2000. The New Zealand Council of Legal Education also requires the general principles and practices of tikanga to be a core component of legal education.[11] In short, tikanga has a well-accepted function within, and influence over, the law in Aotearoa NZ.

Alongside these legal instruments exists a more recent body of work on MDSov and data governance which also draws on tikanga, including:

- Te Mana Raraunga. (2018). *Principles of Māori data sovereignty*.
- Kukutai, Campbell-Kamariera, et al. (2023). *Māori Data Governance Model.*
- Kukutai, Cassim, et al. (2023). *Māori data sovereignty and privacy* (Tikanga in Technology discussion paper).
- Kukutai, Clark, et al. (2025). *Māori Data Privacy Framework.*

[11] The Council instigated regulatory changes to require a compulsory law course on tikanga in the legal education curriculum, as well as the inclusion of relevant content on tikanga in existing compulsory courses. The parliamentary Regulations Review Committee subsequently ruled against the inclusion of tikanga in other core subjects. https://nzcle.org.nz/3.%20Professional%20Examinations%20in%20law%20Regulations%20-%201%20Jan%202025%20updates.pdf

For present purposes we do not need to canvass all this scholarship. However, it is important to describe key tenets of tikanga, its relevance for Māori concepts of privacy and data protection, and the values and practices that a code would need to embody.

Tikanga

Tikanga is the set of values, principles, standards, practices and norms that determine what is considered appropriate or correct in a given context (Durie, 1996). Tikanga guides the way in which relationships are formed and conducted and continues to be practised by Māori communities and institutions. Tikanga includes but extends beyond customary law. As the Law Commission notes:

> The label "law" is unduly narrow, even while tikanga without doubt has legal quality … For similar reasons, we do not use the terms "Māori custom law" or "custom law" – although … custom law is a phrase accurately used to describe one common law category of tikanga recognition. (Law Commission, 2023, pp. 10–11)

Williams (2013) and others (Jackson, 2000; Mikaere, 2007; Quince & Houghton, 2023) have described tikanga as the first law of Aotearoa NZ. This 'first law' status was affirmed by a Supreme Court majority in the 2022 judgment on the high-profile Peter Ellis (*Ellis v R*) appeal case.[12]

Since the 1980s, tikanga has been increasingly woven into statute and the common law. The Law Commission (2023) has identified three categories of tikanga 'claims' in common law: 1) tikanga as custom, 2) tikanga values, and, 3) tikanga as law. Claims based on tikanga as custom seek recognition of a tikanga-based custom or practice as giving rise to legally enforceable rights and interests (p. 225). Claims based on tikanga values typically involve the exercise of weighing of tikanga alongside other values, while tikanga as law claims ask the court to make determinations about tikanga itself.

Unlike tribal (primarily marae-based) kawa which is immutable, tikanga is flexible and responsive to context so can change to meet situational demands. Tikanga evolves over time and is adaptable to wider societal and technological change. In the next section we discuss

[12] *Ellis v R* [2022] NZSC 114

how tikanga regulated the transmission and sharing of information in a customary setting and its application to privacy in a contemporary digital environment.

Tikanga values and privacy

Legal academic Khylee Quince has written at length about tikanga and privacy (Quince, 2016; Quince & Houghton, 2023). Her comprehensive analysis identifies tapu as the primary tikanga underpinning a Māori concept of privacy. Tapu is described as:

> … a Māori concept that defines things that are special or restricted, including the human person, information, places and objects, and indicates sensitivity or risk. The value structure that defines and regulates tapu and other Māori concepts is tikanga. (Quince & Houghton, 2023, p. 44)

Quince and Houghton distinguish between two types of tapu: intrinsic tapu – which is a permanent form of tapu – and temporary tapu. Humans are said to possess intrinsic tapu, which has some resonance with concepts of personal self-worth, respect and dignity. Places such as marae and ancestral burial grounds also have intrinsic tapu. Temporary tapu is a status that exists when a person, place or thing is placed under restriction. This form of tapu can be removed through the process of whakanoa (noa meaning to make something common).

Some forms of knowledge, along with the processes for transmitting or disseminating that knowledge, are considered tapu. Whakapapa, for example, is considered tapu because it connects individuals and their whānau to their ancestors, as well as to all living things, gods and celestial origins. Tohunga have played a central role in safeguarding tapu knowledge and preventing its disclosure to outsiders. Thus, "the tohunga may be viewed as an individual whose role is to hold and regulate collectively private knowledge on behalf of Māori whānau, hapū and iwi" (Quince & Houghton, 2023, p. 56). In a digital environment, some classes of Māori information may have enduring tapu while other kinds of information may only require temporary restrictions, depending on the context.

Quince notes while there is some overlap between Māori and Western concepts of privacy, there are also significant differences, the most obvious being that Māori concepts of privacy are inherently collective. These different cultural concepts of privacy reflect tensions between "Western liberal notions of individualism and the Māori preference for collectivism"

(Quince, 2016, p. 42). A review of Indigenous concepts of privacy by the TiNT team found a number of key shared features:

- Indigenous concepts of privacy are inherently collective, and are underpinned by Indigenous laws and protocols that determine when, how and by whom cultural knowledge, rituals and information can or even should be shared.
- Indigenous privacy is primarily constructed in relation to group interests in relation to cultural practices, values and belief systems.
- Collectives have the right to own information collectively in the same way that an individual owns his or her personal information. This includes the right of control over access and use of knowledge or information that derives from unique cultural histories, expressions, practices and contexts.
- The collective interest may affect not only the individual to whom the information relates, but also the wider group to which the individual may belong.
- Recognising and upholding relationships of belonging, responsibility and respect are paramount. (Kukutai, Cassim, et al., 2023)

For Māori, the collectivist orientation to privacy is rooted in the primacy of whakapapa. Often used synonymously with genealogy, the broader meaning of whakapapa encompasses a vast genealogical sequence that includes flora, fauna, non-living objects and the wider cosmos (Harmsworth & Awatere, 2013; Roberts, 2013). Quince (2016) argues this results in a "different sense of what and where is private and who makes decisions over access to, or sharing of, private information" (p. 42). The marae is illustrative of this point. Quince cites a well-publicised case in which Tūhoe leader Tame Iti was charged with firearms offences after he fired a shotgun at a flag, in protest, on the marae ātea of Tauarau marae. The marae ātea was subsequently identified as a "public place" on the indictment, a designation upheld by the Court.[13] Quince, however, argues that the marae should be considered a private space (and thus be afforded a collective privacy right) except in relation to those who have whakapapa or community links to it. For the latter, the marae functions as a communal public space, with its own kawa and tikanga.

Quince also sees Māori collectivist concepts of privacy as relevant for health information and genetic privacy. In contrast to the Western emphasis on the uniqueness of individuals' DNA

[13] *R v Iti* [2007] NZCA 119, [2008] 1 NZLR 587.

and their personal privacy rights, Māori recognition of shared whakapapa encoded within genetic information raises collective ownership and privacy rights. Thus, for Māori, the unauthorised "use, dissemination and commercial exploitation of genetic material" could be considered as much a breach of collective privacy as individual privacy (Quince, 2016, p. 46). Quince suggests a collective privacy right could also be invoked in instances of group surveillance in tribal territories, as in the case of the 'Urewera raids' (Sluka, 2010), and to protect Indigenous lands from surveillance technologies that aid exploitation.

Māori data sovereignty

In the last decade, the field of MDSov and Indigenous data sovereignty (IDSov) has generated significant scholarship that is also relevant to Māori data privacy considerations (Carroll et al., 2020; Kukutai & Taylor, 2016; Walter et al., 2020). MDSov refers to the inherent rights and interests that Māori individuals, groups and nations have in relation to the collection, ownership and application of Māori data (Te Mana Raraunga, 2018). MDSov is part of a growing IDSov movement that is being pursued by many First Nations Peoples, supported by global human rights instruments such as the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP) and domestic treaties (Carroll et al., 2020; First Nations Information Governance Centre, 2020; Kukutai & Taylor, 2016; Tsosie, 2019).

Standard definitions of Māori data are much broader than the Act's focus on personal information (Kukutai, Cassim, et al., 2023; Te Mana Raraunga, 2018). Māori data refers to digital or digitisable data, information or knowledge (including mātauranga Māori) that is about, from or connected to Māori (Te Kāhui Raraunga, 2021; Te Mana Raraunga, 2018). Māori data includes data about population, place, culture and environment; data generated and shared through government, private sector, civil society and te ao Māori systems and technologies; and mātauranga Māori in all its forms.

Māori data is considered a taonga that is protected under Article 2 of te Tiriti (Te Kāhui Raraunga, 2021a, 2021b; Te Mana Raraunga, 2018). The question of whether something is a taonga is indicative of the strength of the Māori interest and therefore the standard of active protection required of the Crown (Waitangi Tribunal, 2021). A key objective of MDSov is to push back against "data colonialism" (Couldry & Mejias, 2019) and to ensure that Māori data is not colonised in the same way as Māori lands and waterways (Cormack & Kukutai, 2022).

A Māori right to control Māori data is multidimensional. It involves recognising and applying Māori approaches to data, end to end, and over the life cycle of Māori data. This means applying Māori approaches, derived from tikanga, to regulate and govern issues as diverse as:

- how Māori data is to be defined,
- what rules apply to collecting, using and disclosing Māori data,
- who is entitled to assert rights over Māori data and MDSov,
- what safeguards should be employed to oversee and regulate third-party analysis and interpretation of Māori data, and,
- how Māori data should be secured.

It also involves delineating between individual and collective Māori data, both in the context of tikanga and in the context of Western notions applicable to the ownership of information and control over information.

While the Act does not explicitly recognise collective information or a collective privacy right, these are not necessarily mutually exclusive concepts. A collective is simply an aggregation of information held by the individuals who comprise the collective. Although the sum of that information may be greater than its parts, this does not mean that the individual information that forms part of the collective cannot be protected, or that its dual nature precludes individual protections offered under the Act. From a tikanga perspective, some classes of Māori data take on both personal and collective dimensions. The Law Commission recognised this conundrum in its review of the 1993 Act, noting that "individual privacy is connected to the collective, such that individual and collective privacy interests may be mutually reinforcing" (Law Commission, 2010, p. 458).

Māori concerns about privacy

Three key points can be made thus far:

- Māori concepts of privacy differ from Western concepts.
- Tikanga remains relevant in decisions about data protection.
- Collective privacy is important to Māori and ought to be recognised, respected and protected.

These concerns all pose challenges, in different ways, to existing privacy arrangements in Aotearoa NZ. In its reviews of the 1993 Act, the Law Commission (2010) noted that the Act could not readily accommodate the idea of collective or group rights to privacy (p. 460). If

Māori saw certain types of information as belonging to groups rather than individuals, it "may be possible to recognise this belief through areas of law other than privacy law", such as intellectual property rights (Law Commission, 2011, p. 299). Special legal mechanisms could also be created in other legislation for certain types of sensitive information relating to Māori. An example given was the regulations providing for a National Kaitiaki Group to oversee the use of information about Māori women from the National Cervical Screening Register.[14] The Law Commission also noted that the Privacy Commissioner, at the time, did not consider that there were any bicultural issues that needed to be addressed with amendments to the Act. It was up to organisations "to take advantage of the Act's flexibility in order to tailor their practices to meet individual and cultural preferences" (Law Commission, 2011, p. 298).

We think it timely to revisit these assumptions, given the well-documented risks of new data technologies (Curzon et al., 2021; Manheim & Kaplan, 2019; Martin & Zimmermann, 2024), as well as the growing demand by Māori for sovereignty over their data and ongoing privacy concerns. The OPC's most recent biennial privacy report showed that Māori are more concerned than non-Māori about privacy in every aspect (Office of the Privacy Commissioner, 2024). For example, Māori are more likely to be concerned about individual privacy and protection of personal information (59% cf. 51% for the general public), to see children's privacy as a major concern (80% cf. 62%) and have higher levels of concern on a range of privacy issues including facial recognition technology (FRT) and government sharing of data (Office of the Privacy Commissioner, 2024). This is perhaps unsurprising, given well-publicised incidents relating to the unauthorised Police photographing of rangatahi Māori (Office of the Privacy Commissioner and Independent Police Conduct Authority, 2022; Tauri & Deckert, 2022), and concerns about Māori being wrongly identified as shoplifters in a supermarket pilot of FRT (O'Shea, 2024; Paweai, 2024). During the Commissioner's consultation on a Biometric Processing Privacy Code, Māori expressed a range of concerns about biometric data collection and use including cultural harms arising from misuse of Māori biometric information, racial bias and profiling, lack of accuracy leading to misidentification, and surveillance overreach (Office of the Privacy Commissioner, 2023b). It goes without saying that Māori concerns about bias and surveillance are not new. As Quince (2016) argues, the surveillance of Māori, both individually and collectively, is

[14] Health (Cervical Screening (Kaitiaki)) Regulations 1995. The Regulations also specifies the need for "culturally appropriate protection for the taonga of protected information" (s 5(3b)).

situated within a "significant history of surveillance and community intervention directed specifically at Māori" (p. 47).

The Law Commission's 2020 report on the use of DNA in criminal investigations also noted heightened concerns of Māori with privacy and surveillance, particularly given wider perceptions of racism being "embedded in every part of the criminal justice system" (p. 69). Of particular concern was the use of DNA in familial searching – a technique that involves searching the Police's DNA Profile Databank for a near match with a crime scene profile because a direct match has not been obtained (p. iv).[15] The use of DNA in familial searching disproportionately affected Māori adults, given over-representation of Māori on the DNA databank.

Having identified key aspects of Māori perspectives on privacy, and the role of tikanga, we next consider the concept of privacy and what it entails, including the categories of privacy protections generally recognised under Aotearoa NZ law.

[15] The DNA Databank is administered by PHF Science (formerly the ESR) on behalf of the New Zealand Police. https://www.phfscience.nz/news-publications/about-the-dna-databank/

PART 3. PRIVACY

This section is designed to provide a high-level account of privacy and its place within the Aotearoa NZ legal system. It then focuses on the information privacy framework established under the Act and its code-making powers that enable the Privacy Commissioner to modify and shape the protections established under the IPPs to develop codes that might better protect Māori data. Our analysis focuses on what these powers entail and how they can be deployed to provide information privacy protections for Māori that are more closely aligned with the requirements of tikanga.

Privacy: A brief background

WHAT IS PRIVACY?

One of the foundational issues that has inhibited the development of privacy rights is that these have been "seriously handicapped by the lack of a universally agreed and accepted definition of privacy" (Office of the High Commissioner for Human Rights, 2016, p. 9*)*.

Countless attempts have been made to develop a satisfactory definition of privacy. Many are derived from American scholarship and case law beginning in the late nineteenth century, the United States (US) being the first Western common law based country to develop a tort of privacy infringement, accompanied by a range of cognate tortious remedies.

The origins of the concept of privacy within these traditions are generally traced back to an article written by Samuel Warren and Louis Brandeis in 1890, "The Right to Privacy", where they define privacy as "the right to be let alone" (Warren & Brandeis, 1890, p. 193). They build their argument in support of this concept by reference to a pervasive theme in privacy discourse – the encroachment of technology on the private sphere. Their preoccupations focused on late nineteenth century incursions on solitude and "inviolate personality" attributable to "invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sounds" (p. 205). Concerns about the effect of technology, primarily the internet and associated technologies, on a right to be let alone are a continuous preoccupation of contemporary privacy scholarship and advocacy.

A variety of researchers have sought to elaborate on privacy as a right to be let alone, many noting that such a conceptualisation does not account for the variety of instances where individuals seek to limit access to themselves or information about them. Some have attempted to develop a single unified 'theory' of privacy that accounts for all its possible dimensions. However, as Robert Post (2001, p. 2087) has stated, "Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can usefully be addressed at all."

Putting aside whether a single, unified conceptualisation of privacy is possible, Daniel Solove has developed one of the most widely accepted approaches to privacy. He takes a pragmatic definitional approach that locates privacy within a taxonomy consisting of six elements "which capture the recurrent ideas in the discourse" about privacy as follows:

> (1) the right to be let alone – Samuel Warren and Louis Brandeis's famous formulation for the right to privacy; (2) limited access to the self – the ability to shield oneself from unwanted access by others; (3) secrecy – the concealment of certain matters from others; (4) control over personal information – the ability to exercise control over information about oneself; (5) personhood – the protection of one's personality, individuality and dignity; and (6) intimacy – control over, or limited access to, one's intimate relationships or aspects of life. (Solove, 2002, p. 1092)
>
> There are certain similarities in particular types of disruptions (of privacy) as well as in the practices that they disrupt; but there are differences as well. We should conceptualize privacy by focusing on the specific types of disruption and the specific practices disrupted rather than looking for the common denominator that links all of them. If privacy is conceptualized as a web of interconnected types of disruption of specific practices, then the act of conceptualizing privacy should consist of mapping the typography of the web. (Solove, 2002, p. 1130)

Outside these categories of rights, there are other approaches to defining privacy. One draws on human rights law, often referred to as 'fundamental rights and freedoms', where privacy is considered to be an "enabling right" that facilitates "the enjoyment of other rights: the free development and expression of an individual's personality, identity and beliefs, and their ability to participate in political, economic, social and cultural life" (Office of the High Commissioner for Human Rights, n.d.).

Aotearoa NZ law recognises some of the elements of Solove's typography of privacy rights through a patchwork of legal protections. These legal protections consist of the Act, which covers the fourth category of Solove's taxonomy – control over personal information about oneself, which is commonly referred to as 'information privacy' – as well as common law rights to privacy.[16]

Privacy in Aotearoa NZ

The Bill Of Rights

The Bill of Rights Act 1990 (Bill of Rights) does not include a right to privacy although there are some privacy protections in respect of unreasonable search and seizure.[17] However, the absence of a right to privacy in the Bill of Rights does not mean that any existing rights or freedoms are abrogated or restricted by not having been included in it.[18]

Privacy At Common Law

One of those existing rights is common law privacy rights. A tort of invasion of privacy was first recognised by the Court of Appeal in *Hosking v Runting* [2005] 1 NZLR 1 (CA). The Court decided that in order to make a successful invasion of privacy claim, two elements need to be established: (1) the existence of facts in respect of which there is a reasonable expectation of privacy, and (2) that publicity is given to those facts that would be considered highly offensive to an objective reasonable person.

Subsequent jurisprudence has recognised that common law privacy rights also encompass a right against an intrusion into seclusion. In *C v Holland* [2012] NZHC 2155, the Court stated that the elements of this cause of action are: (1) an intentional and unauthorised intrusion; (2) the intrusion must be into seclusion such as an intimate personal activity, space or affairs; (3) that the intrusion involves an infringement of a reasonable expectation of privacy; and (4) the intrusion is of a nature as to be highly offensive to a reasonable person.

Both of these common law privacy rights are focused on individual not collective rights. That said, the common law is flexible and can evolve through case law to cover new or emerging

[16] For the sake of completeness, there are a variety of statutory provisions, including laws about search and seizure, that can be said to protect certain privacy rights. These are not covered in this paper as its focus is on the Act's code-making powers.

[17] Bill of Rights Act 1990, s 21.

[18] Section 28.

areas of law and legal liability. The tort of privacy itself is a good example of this. Before *Hosking v Runting* it was thought that the only privacy rights in Aotearoa NZ were those established under the now-repealed Privacy Act 1993. Using the common law to better protect Māori data through test cases and representative proceeding litigation is an option for Māori that deserves further exploration but is beyond the scope of this paper.

THE PRIVACY ACT 2020: INFORMATION PRIVACY IN AOTEAROA NZ

Information privacy in Aotearoa NZ is regulated by the Privacy Act 2020.

Under normal statutory interpretation rules, legislation must be interpreted consistently with its purposes unless there is some other recognised reason, such as the explicit text of the legislation, to take a different approach.

The Act's purposes are set out in s 3:

> The purpose of this Act is to promote and protect **individual privacy** by—
>
> (a) 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
>
> (b) 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. (our emphasis)

The Act thus has dual purposes: the first is to protect individual privacy while balancing that right against other countervailing interests, and the second is to give effect to international privacy obligations and standards. These purposes need to be taken into account when the Commissioner considers exercising code-making powers.

Balancing the individual privacy right against other countervailing interests can lead to disclosure of the personal information, even if in conflict with tikanga principles, provided the circumstances justify disclosure. [19]

[19] In *Te Pou Matakana Limited v Attorney-General* [2021] NZHC 3319, when considering whether the right of privacy took precedence over the right of a health provider to access health information, Dr Carwyn Jones stated that "Where that taonga is at risk, not all tikanga principles, values or practices will be able to be perfectly fulfilled, and where certain aspects of tikanga conflict with the purpose of protecting health, there is little expectation that they will be pursued at the cost of the caring for the health and wellbeing of whakapapa."

Subsection 3(b) refers to international obligations and standards, making explicit reference to the OECD Guidelines. These are defined in s 7 of the Act as being "the Organisation for Economic Co-operation and Development Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data".

The OECD Guidelines

The *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines) were first published in 1980 and subsequently updated in 2013. Although not having the status of international law, they "represent the first internationally agreed-upon set of privacy principles" and "since their adoption, they have influenced legislation and policy in the OECD and beyond" (p. 3). They consist of a set of eight principles that govern the collection, use, disclosure, security and other handling of personal information and have formed the basis for many information privacy laws across the world, including the Act and its IPPs. The OECD guidelines apply to "personal data" which is defined to mean "any information relating to an identified or identifiable individual" (p. 6). The OECD Guidelines expressly apply to *personal* information privacy. They do not cover or refer to collective rights and thus do not provide a means by which a collective right to privacy could be supported under the Act.

The scheme of the Act

As noted in this paper's introduction, the definition of 'personal information' is set out in s 7 of the Act. The same section defines an individual to be "a natural person, other than a deceased natural person". While the focus of the Act is on regulating the information privacy of living individuals, it can extend to information about a deceased person but only where that information is in the Register of Deaths.

Central to the Act's principles-based approach are the IPPs set out in s 22 of the Act. The 13 IPPs establish rules that govern the collection, use, disclosure, security, access, correction, accuracy and other handling of personal information by agencies. The Act does not delineate between personal information and sensitive information.[20] The protections in the IPPs apply to all types of personal information in the same way. This uniform approach to all categories of personal information regardless of their sensitivity differs from information privacy

[20] OPC has published a note/explainer on sensitive personal information and the Act: https://www.privacy.org.nz/assets/New-order/Your-responsibilities/Privacy-resources-for-organisations/Sensitive-Personal-Information-and-the-Privacy-Act-2020.pdf

legislation in other jurisdictions where sensitive information – such as health, sexuality, ethnicity, religion, political or religious affiliation, criminal record, and genetic and biometric information – are given additional protection.[21] The European Union's *General Data Protection Regulation* (GDPR), for example, treats health and genetic data as sensitive data and the processing of such data is prohibited unless specific conditions are met, such as an individual gives explicit consent to do so.

All agencies, as defined in s 8 of the Act, are required to comply with the IPPs. In broad terms an agency is an individual not acting in a domestic capacity, public sector organisations and private sector organisations.

The Act protects against the interference with the privacy of an individual. Such an interference occurs where the action of an agency breaches one or more of the IPPs in relation to the individual *and* causes, or may cause, "loss, detriment, damage or injury to the individual",[22] or has "adversely affected, or may adversely affect, the rights, benefits, privileges, obligations or interests of the individual",[23] or " has resulted in, or may result in, significant humiliation, significant loss of dignity, or significant injury to the feelings of the individual".[24]

The Act enables individuals who are aggrieved by an interference with their privacy to make a complaint to the Commissioner.[25] The Act does not therefore confer a direct right of action on an individual to seek redress for an interference with privacy. For example, an individual who considers that their personal information has been collected unlawfully or unfairly in breach of IPP 4 cannot initiate legal proceedings against the agency alleged to have done so.

Pausing at this point, there are a number of key points to note.

The first is that the Act is only concerned about information privacy. Although information privacy is an important component of an overall privacy right, it is – as noted earlier – only one dimension of it.

---

[21] By way of contrast, art 9 of the EU's *General Data Protection Regulation* (EU Regulation 2016/679) provides additional protections for "special categories of personal data". These are commonly referred to as 'sensitive information'. In Australia, s 6 of the Privacy Act 1988 (Cth*)* defines sensitive information and the Australian Privacy Principles (APPs) confer additional protections on sensitive information.

[22] Privacy Act 2020, s 69(b)(i).

[23] s 69(b)(ii).

[24] s 69(b)(iii).

[25] s 71.

The second is that the overwhelming emphasis in the Act is on **individuals'** information privacy. Its overall purpose, its key definitions, and the IPPs themselves focus on the personal dimensions of information privacy. The Act does not refer to collective rights in Māori information and does not provide any explicit mechanism for protecting collective rights.

The third is that the rights conferred by the Act are not rights that individuals can enforce themselves – they can only be enforced on complaint to the Commissioner, as a gateway to bringing proceedings in the Human Rights Review Tribunal if the complaint is not resolved. As such, information privacy rights in New Zealand are *mediated rights*; that is, individuals cannot themselves enforce information privacy rights. Rather, if not resolved after first raising the complaint with the relevant party directly, they must lodge a complaint to the Commissioner, and the Commissioner must then decide to initiate some type of action under the complaints investigation and dispute resolutions functions.

The fourth is that for the Commissioner to investigate action for an interference with privacy, the Commissioner must be satisfied of two things: that a breach of the IPPs may have occurred *and* that some form of loss may have occurred. There are two exceptions.[26]

The fifth is that the Act regulates all personal information equally. Sensitive personal information is not given additional protection. This is problematic for Māori because some information is considered to be highly sensitive, including personal information about spiritual and cultural practices, whakapapa, and information relating to death and the deceased.

These five issues significantly limit Māori privacy rights under the Act. Even where Māori wish to enforce their personal information rights, they cannot do so directly. Their autonomy is attenuated because their rights can only be enforced through the Commissioner and are subject to the Commissioner's gatekeeping role.

In view of these significant limitations, we now turn to consider whether the code-making provisions can address these limitations in a way that is more compatible with tikanga.

[26] The exceptions are an individual's right to obtain access to their personal information held by an agency under IPP 6 and an individual's right to correct personal information held by an agency under IPP 7.

Codes of Practice

As noted earlier, the Commissioner's code-making powers are set out in Part 3 subpart 2 of the Act. Codes introduce a measure of flexibility into the Act. A code can provide additional protections for higher-risk categories of personal information or privacy intrusive activities. The code-making powers enable the Commissioner to modify the application of one or more of the IPPs.[27] Among other things, the Commissioner may develop special rules for particular classes of information and to tailor the Act's protections to address particular categories of information privacy risks. Under the code-making powers, the Commissioner is able to both increase and/or reduce levels of information privacy protection in the IPPs.

The code-making powers have been exercised by the Commissioner to provide more appropriate information privacy rules for specific information privacy risks, circumstances, classes of information, types of agency and types of activities.

Some examples of codes issued by the Privacy Commissioner are for:

- credit reporting,[28]
- telecommunications,[29]
- health information,[30] and
- superannuation schemes unique identifiers.[31]

A Biometric Processing Privacy Code was issued in August 2025, with the new rules coming into effect in November 2025.

The Commissioner states that code provisions are designed to enable the Commissioner to "**modify the operation of the Privacy Act** and set rules for specific industries, organisations, or types of personal information"[32] (our emphasis). Although a code, once developed under

[27] However, the code provisions do not permit the Commissioner to limit or restrict individuals' rights to access or correct their personal information. See Privacy Act 2020, s 32(5).

[28] Credit Reporting Privacy Code 2020. https://www.privacy.org.nz/assets/New-order/Privacy-Act-2020/Codes-of-practice/Credit-reporting-privacy-code-2020/Credit-Reporting-Privacy-Code-2020-website-version.pdf

[29] Telecommunications Information Privacy Code 2020. https://www.privacy.org.nz/assets/New-order/Privacy-Act-2020/Codes-of-practice/Telecommunications-information-privacy-code-2020/Telecommunications-Information-Privacy-Code-2020-website-version.pdf

[30] Health Information Privacy Code 2020. https://www.privacy.org.nz/assets/New-order/Privacy-Act-2020/Codes-of-practice/Health-information-privacy-code-2020/HIPC-Amendment-No-1/Consolidated-Code-incorporating-Amendment-No-1.pdf

[31] Superannuation Schemes Unique Identifier Code 2020. https://www.privacy.org.nz/assets/New-order/Privacy-Act-2020/Codes-of-practice/Superannuation-schemes-unique-identifier-code-2020/Superannuation-Schemes-Unique-Identifier-Code-2020-website-version.pdf

32 https://www.privacy.org.nz/privacy-act-2020/codes-of-practice/

the Act, has the effect of modifying its operation, the Commissioner's code-making powers are not a power to rewrite the Act; rather, these powers are constrained by the express words of the Act.

THE CODE-MAKING POWERS

Section 32 of the Act states that:

> (1) The Commissioner may at any time issue a code of practice **in relation to the IPPs**.
>
> (2) A code of practice may—
>
> (a) **modify the application of 1 or more of the IPPs** by—
>
> (i) prescribing more stringent or less stringent standards:
>
> (ii) exempting any action from an IPP, either unconditionally or conditionally:
>
> (b) apply 1 or more of the IPPs without modification:
>
> (c) prescribe how 1 or more of the IPPs are to be applied or complied with.
>
> (3) A code of practice may apply in relation to 1 or more of the following:
>
> (a) **any specified information or class or classes of information**:
>
> (b) any specified agency or class or classes of agency:
>
> (c) any specified activity or class or classes of activity:
>
> (d) any specified industry, profession, or calling or class or classes of industry, profession, or calling. (our emphasis)

One of the limitations that the code-making powers impose on the Commissioner is that a code must be "in relation to the IPPs" and that a code may "modify the application of 1 or more of the IPPs."[33] The code-making powers are thus limited to the IPPs (i.e., to s 22 of the Act) and are not a power to modify or alter other provisions of the Act such as its purposes, its definitions, or its provisions that establish the office of the Commissioner and complaints-handling.

WHAT MUST THE COMMISSIONER CONSIDER WHEN EXERCISING CODE-MAKING POWERS?

In considering whether to exercise code-making powers and how to exercise them, the Commissioner is required to have regard to the express words of the code-making grant of powers. In addition, as those powers are discretionary, the Commissioner is also required to

[33] Note, however, that the Code-Making power can modify the definition of 'individual' in s 7 of the Act to extend to deceased persons: see s 32(6) of the Act.

have regard to any other provisions of the Act that apply to how that discretion should be exercised as well as general law statutory interpretation rules.

One of the statutory interpretation requirements is the Act's purposes clause, s 3 of the Act, which is referred to earlier.

Another is s 21 of the Act, which contains explicit provisions that require the Commissioner to take account of certain matters when exercising a statutory power, including the code-making powers. Section 21 states:

> **Commissioner to have regard to certain matters**
>
> The Commissioner must, in performing any statutory function or duty, and in exercising any statutory power,—
>
> (a) have regard to the **privacy interests of individuals** alongside other human rights and interests, including—
>
> (i) the desirability of facilitating the free flow of information in society; and
>
> (ii) government and businesses being able to achieve their objectives efficiently; and
>
> (b) take account of international obligations accepted by New Zealand, including those concerning the international technology of communications; and
>
> (c) **take account of cultural perspectives on privacy**; and
>
> (d) consider any developing general international guidelines relevant to the better protection of **individual privacy**; and
>
> (e) have regard to the IPPs. (our emphasis)

The code-making powers and international obligations

International law

The right to privacy is recognised as a fundamental right under international human rights law. Article 12 of the *Universal Declaration of Human Rights* (Declaration) states that:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR)[34] confers a right to privacy in similar, but not identical, terms:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

As confirmed by the United Nations Human Rights Council in Resolution 28/16, The right to privacy in a digital age, both the Declaration and the ICCPR constitute the basis of the right to privacy in international law. As a member of the United Nations, Aotearoa NZ is bound by the Declaration. It is also bound by the ICCPR, having ratified it on 28 December 1978. As international law, both are clearly "international obligations" the Commissioner should consider.

Both Article 12 of the Declaration and Article 17 of the ICCPR are concerned with the rights of individuals and do not provide a basis for a code that would protect a collective right to privacy. Another international obligation is the *United Nations Declaration on the Rights of Indigenous Peoples* (UNDRIP).

United Nations Declaration of the Rights of Indigenous Peoples

The UNDRIP was adopted by the General Assembly in 2007. New Zealand was one of only four member States that voted to oppose the Declaration,[35] but in 2010 New Zealand reversed its position and notified the UN of New Zealand's support for the Declaration.[36, 37]

As a General Assembly Declaration, UNDRIP does not neatly fall within the categories set out in s 21 of the Act. Subsection 21(b) of the Act refers to "international obligations" as being relevant to the exercise of the Commissioner's powers. Our interpretation of this provision is that if s 21 had meant to only cover international law it would have said so. The

[34] We note that Article 16 of the *United Nations Convention on the Rights of the Child* (UNCRC) stipulates: "No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation".

[35] The others were Australia, Canada and the US.

[36] New Zealand Government. (2010, 20 April). *Supporting UN Declaration restores NZ's mana.* https://www.beehive.govt.nz/release/supporting-un-declaration-restores-nzs-mana

[37] New Zealand Government. (2010, 20 April). *Mihi to United Nations Permanent Forum on Indigenous Issues, Announcement of New Zealand's Support for the Declaration on the Rights of Indigenous Peoples*. https://www.beehive.govt.nz/sites/default/files/100420_UNDRIP.pdf

use of "international obligations" implies a broader scope that can encompass obligations that extend beyond international law obligations.

UNDRIP is the authoritative international legal instrument that guides the way in which States should engage with and protect the rights of Indigenous people. As a UN General Assembly Declaration, it does not, on its own, constitute international law except to the extent that individual articles within it can be considered to reflect international law either through a Treaty or customary international law. One of its articles, Article 3, which states that "Indigenous peoples have the right to self-determination", is clearly international law as it is consistent with the right to self-determination set out in Article 1 of the ICCPR. Importantly, this right is a *collective right* that vests in groups – peoples – and not just in individuals.

Article 31 of UNDRIP specifically addresses Indigenous peoples' rights to protect traditional knowledge:

> **Article 31**
>
> 1. Indigenous peoples have the right to maintain, control, protect and develop their cultural heritage, traditional knowledge and traditional cultural expressions, as well as the manifestations of their sciences, technologies and cultures, including human and genetic resources, seeds, medicines, knowledge of the properties of fauna and flora, oral traditions, literatures, designs, sports and traditional games and visual and performing arts. They also have the right to maintain, control, protect and develop their intellectual property over such cultural heritage, traditional knowledge, and traditional cultural expressions.
> 2. In conjunction with indigenous peoples, States shall take effective measures to recognize and protect the exercise of these rights.

Māori collective information and principles of MDSov to protect them clearly fall within the ambit of the protections conferred under Article 31 of the Declaration. It follows that the Commissioner can properly have regard to it in exercising the code-making powers.

Other international guidance

Privacy law evolves primarily because of rapid technology developments. Many international organisations develop and publish proposals for reform to address these technological impacts. At present, there is significant activity in the area of the impact of AI and privacy. For example, the OECD has developed a set of AI principles that are the first

intergovernmental standard on AI and that include references to better privacy protections for the use of personal data in various types of AI.[38] There are also the G20 AI Principles, also developed in 2019, that identifies (among other things) privacy issues in relation to AI. The United Nations Educational, Scientific and Cultural Organization's (2021) *Recommendation on the Ethics of Artificial Intelligence* highlights the importance of privacy for the protection of human dignity, autonomy and agency.

[38] See, in particular, Principle 1.2.

PART 4. A MĀORI DATA CODE

There is no in-principle reason that prevents the Commissioner from developing a code that could make the Act more protective for Māori, by providing additional protection over classes of information that are regarded as tapu, and having regard to its cultural significance and the principles set out in UNDRIP. The notion of applying tikanga to privacy approaches involving culturally significant information is not new. As the Law Commission noted in 2008, "Te ao Māori is an important dimension of the New Zealand social fabric, and should be reflected in our legal treatment of privacy" (p. 16). More recently, the (now disestablished) Government Chief Privacy Officer advised Government that tikanga should be applied when agencies were proposing to share Māori data and information, as well as to its subsequent use. This consideration was especially important when developing an information-sharing agreement with a Māori organisation, iwi or hapū (Government Chief Privacy Officer, 2024).

The Act already covers the personal information of Māori individuals in the same way it does any other individual. Some of these considerations for Māori can be addressed in a code but others cannot. For a code to work, it would need to offer additional protection – especially, we argue, tikanga-based protection – for particular classes of sensitive personal information.

What classes of Māori data could be protected under a Code?

In considering this question, we can look to recent statements from the Office of the Privacy Commissioner (OPC) about Māori privacy considerations. In a discussion document on a potential biometric processing code, the OPC noted:

> Biometric information is of particular cultural significance to Māori. During OPC's consultation in 2022, we heard from Māori that biometric information is related to whakapapa and carries the mauri of the individual it was taken from. As such it is tapu to the individual, their whānau, hapū and iwi and should be protected as a taonga in accordance with tikanga and mātauranga Māori. This status has implications for the collection, storage, use and disposal of biometric information and for consultation with Māori in the development of biometric projects. (Office of the Privacy Commissioner, 2023a, p. 8)

In a panel on tikanga and privacy held for Privacy Week 2022, the Deputy Commissioner noted that the OPC was keen to better understand what privacy means from a te ao Māori

lens. Rather than translate the Act into Māori terms, the OPC wanted to understand how tikanga applied to Māori concepts of privacy and the protection and safe use of information (quoted in Quince & Houghton, 2023, p. 125).

Where tikanga has been specified in legislation, it has been to make a requirement or provision for tikanga values and practices, rather than to narrowly codify what or how tikanga should be applied in a given context. In a similar fashion, it may be that a Māori data code would not prescribe how tikanga should be interpreted or applied in relation to specific classes of Māori data, but rather require that its collection use, disclose, security and handling be consistent with tikanga. Drawing on our reading of the literature, we focus here on the tapu or restricted classes of sensitive Māori data that a code might cover. The aim is not to lock down Māori data, but rather to ensure that it is collected, shared, disclosed and so forth in a way that is 'tika' or correct according to Māori values.

WHAKAPAPA DATA

There is ample evidence of the need for legislation to be more protective of whakapapa data. For data to be within the scope of the Act, it must be personal data, thus excluding whakapapa data relating to places and territories, non-human life forms and mātauranga Māori. In a digital context, human whakapapa data includes any data that links individuals to their kin, including genetic and genealogical data.

DNA

DNA data are some of the most sensitive forms of data and contain large amounts of unique information. DNA are 'extra-individual' in that the data not only carries the unique genetic blueprint of a person but also reveals something about others to whom they are biologically related (Gomberg, 2023). The Law Commission (2020) states: "DNA contains whakapapa (genealogy) information, which is considered to be taonga, and some consider human tissue and DNA themselves to be taonga" (p. 58). Quince and Houghton (2023) concur: "For Māori, DNA represents the individual, their whānau, hapū and iwi, and their whakapapa. DNA is a taonga and any DNA collection should be carried out in accordance with tikanga" (p. 86).

An important consideration is whether genetic information can be used alongside other information to identify a relative (i.e., someone other than the person from whom the genetic information derives). From a tikanga perspective, shared rights and interests can be recognised and the weighing of those rights would need to balance against the purpose for which the DNA is to be used. In its 2020 report, the Law Commission recommended that new

DNA legislation should recognise that tikanga may be engaged by "various aspects of the regime" and make provision for its operation, where appropriate. It also recommended regulation of the use of genetic genealogy searching in criminal investigations.

Forensic genetic genealogy (FGG) or forensic investigative genetic genealogy (FIGG) is a tool that is primarily used by law enforcement, particularly in the US. It involves more distant familial identification, rather than a search for a direct match with the actual suspect. Law enforcement agencies test a crime scene, obtain a DNA sample, and then upload the data (usually a single nucleotide polymorphism (SNP) profile) to a commercial database where others have voluntarily shared their data from consumer DNA testing companies in order to find relatives. Law enforcement can use these databases to find relatives – including quite distant ones – of the unknown person whose DNA was collected from the crime scene. In the case of the notorious Golden State Killer Joseph DeAngelo, law enforcement used FIGG to identify individuals who were the equivalent of third cousins, and then incorporated other information from record searches, including genealogical records, to successfully narrow down their search. Their search involved relatives who had never submitted DNA to a genetics service, raising questions about ethical use of genetic data and informed consent (Berkman et al., 2018).

The use of FIGG is not confined to the US. In 2023, the NZ Police and Environmental Science and Research (ESR) began a trial of a FIGG for 'cold cases'. ESR uploaded SNP profiles to GEDmatch PRO, a genetic database hosted in the US which has the option to be utilised for law enforcement purposes. The Police website notes, "Results from genealogy websites, where submitters provide law enforcement access to their records, are used as the basis of genealogy searching of publicly available records such as genealogy database, church records and libraries."[39] It does not refer to reference testing – when law enforcement requests a DNA sample from a person in a partially constructed family tree using FIGG. It is unclear, from the ESR or Police websites, whether the pilot has concluded, ceased or been fully implemented.

The use of tapu data, in the form of both DNA and genealogical data, in criminal investigations raises a number of issues requiring tikanga consideration. From a tikanga perspective, it is critical that its use can be justified, while taking account of the public interest in the resolution of serious crime. The Law Commission thus states that, "It is

[39]Accessed 30 September 2025: https://www.police.govt.nz/news/release/genetic-testing-could-provide-leads-cold-cases

important from a tikanga perspective that intrusions upon personal tapu are for good reasons and that those affected understand what is happening and why" (Law Commission, 2020, p. 69). Regarding the sampling of close relatives in criminal investigations, it questioned whether "a relative can give valid consent to the use of their DNA for the purposes of inculpating or exculpating another person" (p. 292).

A Māori data code could offer additional protections for DNA data involving Māori by placing limitations on the purpose and manner of its collection. This would require the exercise of the Code-making powers to modify the effect of IPPs 1 – 4 to ensure that such collection conformed with tikanga values. Corresponding code-based amendments would also need to be considered to provide corresponding use and disclosure protections over DNA data, its security under IPP 5 and, to better conform with tikanga values expressed through MDSov principles to ensure that DNA data remains in Aotearoa NZ. We note that DNA data was out of scope of the Biometric Processing Privacy Code.

Genealogical data

Genealogical data broadly refers to information about an individual's family lineage and the relationships between members. It may be historic or current and can extend from two to many generations. Like DNA, genealogical knowledge is also considered tapu, with restrictions on access. In practice, tikanga in relation to whakapapa information in a digital environment may only be loosely observed.

In Aotearoa NZ, the records of the Māori Land Court hold a large volume of historical whānau, hapū and iwi genealogical data, much of which is open access, in either hard copy or digital form. The information tends to be preserved as lists of owners and successions, and fragments recorded in land court hearings, rather than unified multi-generational family trees. There is also a large volume of whānau genealogical data on commercial and genealogical websites, most of which are commercialised on a pay-for-service subscription. Commercial genealogical websites like Ancestry.com primarily source their data through the digitisation of official records (e.g., births, deaths, marriages, census records) and user-generated content (e.g., family trees). Some websites ask individuals to obtain consent from living relatives before adding them to family trees, but it is unclear whether and how widely this is enforced.

Genealogical data is also collected by government agencies. In the case of Oranga Tamariki (OT), the agency responsible for child care and protection, whakapapa information is centred on the child in its care. Whakapapa is described in s 2 of the Oranga Tamariki Act 1989 as

"the multi-generational kinship relationships that help to describe who the person is in terms of their mātua (parents), and tūpuna (ancestors), from whom they descend". The agency instigates a "whakapapa research process" in a variety of situations including:

- to support whānau engagement with disconnected whānau
- to prevent tamariki coming into care by supporting and preferencing whānau placements
- when a hui ā-whānau is unable to proceed effectively without further research of whakapapa, and
- when there is a need to increase cultural connections for the tamaiti (child) and to support their sense of belonging, identity, self-esteem and overall oranga.[40]

Whakapapa research is meant to be conducted by experienced Māori practitioners who are skilled in applying tikanga Māori and using Māori models of practice to explore and validate whakapapa kinship relationships, but not all Oranga Tamariki sites have this expertise available. The usual practice is to identify three generations for the genogram recorded on the agency's case recording system CYRAS (Care and Protection, Youth Justice, Residential, and Adoption System), which can then be extended out to include aunts, uncles, cousins and others. Only the genograms (3 generations of information) is meant to be kept within OT system, with all other whakapapa information returned to whānau.

DATA ABOUT THE DECEASED

The vexed matter of whether deceased persons (not just Māori) have privacy rights was of sufficient general interest that it had its own section in the Law Commission review of the 1993 Act. In te ao Māori, it is clear that the mana and reputation of an individual does not end in death but carries on in whakapapa.[41] The Law Commission has acknowledged that "there is some evidence that Māori beliefs may recognise a right to protection of deceased individuals' privacy and reputation" (Law Commission, 2010, p. 67). Quince and Houghton (2023, p. 68) are less ambiguous, arguing that, "In the Māori worldview, deceased persons

[40] See https://practice.orangatamariki.govt.nz/core-practice/working-with-maori/how-to-work-effectively-with-maori/whakapapa-research

[41] As confirmed in paragraph 106(c) in the Statement of Tikanga written by Tā Moko Mead and Tā Temara in *Ellis v R* [2022] NZSC 114, which reads "The mana of a person and the associated collectives to which they belong continues when someone dies".

possess dignity and privacy that may be breached." We agree that, from a tikanga perspective, deceased individuals have a right to privacy.

In general, the Act does not apply to deceased people, with s 7 defining "individual" to mean "a natural person, other than a deceased natural person". Thus, except under some very specific circumstances, deceased individuals are not recognised as having an information privacy interest under the Act.

However, the Commissioner's Code making powers under s 32 (6) of the Act enable a sector-specific code of practice to be issued in relation to deceased persons:

> (6) Despite the definition of the term individual in section 7(1),—
>
> (a) a sector-specific code of practice may be issued that applies 1 or more of the IPPs to information about deceased persons (whether or not the code also applies 1 or more of the IPPs to other information); and
>
> (b) the code of practice has effect under section 38 as if those IPPs so applied, and the provisions of this Act apply accordingly.

The effect of these provisions is that protections consistent with those identified by both the Law Commission and Quince and Houghton could be developed under a Code of Practice should the Commissioner choose to do so.

Currently, some Acts, such as the Coroners Act 2006, involve the disclosure of information about the deceased. For example, in coronial inquests in cases involving unexplained sudden death, such as homicide or suicide, the report will be made public. Māori are over-represented in both these types of sudden deaths. By contrast, the banking sector tends to approach the disclosure of personal financial information of deceased individuals in much the same way as living individuals.

A code could make provision for tikanga to be considered in the disclosure of information relating to deceased individuals that would result in whakamā or distress to living uri or descendants, without a clear public benefit. This would likely need to be defined within a specified privacy window (e. g., within X years of death) to be workable and meaningful. We note that a precedent of sorts has already been laid set with Rule 11 of the Health Information Privacy Code (Office of the Privacy Commissioner, 2020) which applies to health information about living or deceased persons obtained before or after the commencement of

the code (Rule 11, clause 6) for a period of up to 20 years (Rule 11, clause 7). Section 9(2)(a) of the Official Information Act 1982 can also be used to protect the privacy of the deceased and their surviving family members (Office of the Ombudsman, 2020).

Where to from here?

Our view is that the Act's code-making powers are sufficiently broad to enable the development of a code that provides better protection for Māori data. We believe there are sufficient grounds for the OPC to begin its own considerations on whether a Māori data code is needed, and what it might entail. The Crown has a duty, arising from Article 2 of te Tiriti, to actively protect data that is considered a taonga, and this includes information that Māori consider tapu or in need of some form of restriction. A code could both recognise and provide for tikanga and te Tiriti in ways that are meaningful and speak directly to the specific privacy concerns that have been expressed by Māori for nearly two decades. Through a tikanga-centred approach, the code could do a number of things in relation to particular classes of sensitive Māori data, including:

- restricting how sensitive classes of Māori information can be collected, used, disclosed, retained, stored and disposed of,
- putting stronger requirements on agencies to demonstrate that their collection, use and disclosure of these classes of Māori information is justified,
- requiring free, prior and informed consent for its use and disclosure, and
- requiring greater transparency and independent oversight, from Māori.

While a code cannot create new privacy rights under the Act – such as a collective privacy right – it could be used to better codify the collection, use and disclosure of personal information for collective purposes and collective benefit. For example, family group conferences are a legislated process under the Oranga Tamariki Act 1989, in which information about the child and their whānau is shared. A former Commissioner noted the expectation of a collective privacy interest in the personal information of children in care. Thus, "Often we see an assumption that extended whānau, such as aunties and cousins, should be involved in the child's care and, therefore, are entitled to information" (quoted in Quince & Houghton, 2023, p. 122).

While we are concerned specifically with privacy issues in relation to special classes of Māori data, we think the issues raised are of wider relevance to all New Zealanders.

In progressing these issues, it will also be important for Māori to carefully consider the cultural implications of any decision to advocate for a Māori data code under the Act. Although we believe that there is scope for this to occur, it is important to be aware that using statutory information privacy mechanisms has limitations and could also lead to unintended consequences. Information privacy rights are not absolute and relying on them could result in a misalignment between tikanga and more limited Western and individualistic notions of information privacy. We have referred to other potential issues earlier in this paper. For example, is it appropriate, in effect, to hand control over the enforcement of Māori data privacy rights to a third party – the Commissioner? Other traditional rights over information that is best characterised as traditional knowledge rather than personal information might better be advanced using the common law or through specific *sui generis* legislation that establishes bespoke rights that are more akin to intellectual property rights than significantly weaker information privacy rights. Determining the right approaches to these complex cultural issues is necessary to ascertain what strategies Māori employ to protect traditional rights in a pervasively digital world.

References

Benton, R., Frame, A., & Meredith, P. (Eds.). (2013). *Te mātāpunenga: A compendium of references to the concepts and institutions of Māori customary law*. Victoria University Press.

Berkman, B., Miller, W. K., Grady, C. (2018). Is it ethical to use genealogy data to solve crimes? *Annals of Internal Medicine*, *169*(5),333–334. http://dx.doi.org/10.7326/M18-1348

Carroll, S. R., Garba, I., Figueroa-Rodríguez, O. L., Holbrook, J., Lovett, R., Materechera, S., Parson, M., Raseroka, K., Rodriguez-Lonebear, D, Rowe, R., Sara, R., Walker, J. D., Anderson, J., & Hudson, M. (2020). The CARE principles for Indigenous data governance. *Data Science 19*(43), 1–12. https://doi.org/10.5334/dsj-2020-043

Coates, N. (2017). The recognition of tikanga in the common law of New Zealand. *Te Tai Haruru. Journal of Māori and Indigenous Issues, 5,* 25–58. https://www.nzlii.org/nz/journals/TaiHaruruJl/2017/5.html

Cormack, D. & Kukutai, T. (2022). Indigenous peoples, data and the coloniality of surveillance. In A. Hepp, J. Jarke & L. Kramp (Eds.), *The Ambivalences of Data Power: New perspectives in critical data studies* (pp. 121-141). London: Palgrave Macmillan.

Couldry, N., & Mejias, U. A. (2019). Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media*, *20*(4), 336–349. https://doi.org/10.1177/1527476418796632

Curzon, J., Kosa, T. A., Akalu, R., & El-Khatib, K. (2021). Privacy and artificial intelligence. *IEEE Transactions on Artificial Intelligence*, *2*(2), 96-108.

Durie, E. (1996). Will the settlers settle? Cultural conciliation and the law. *Otago Law Review, 8*, 449–465. https://www.nzlii.org/nz/journals/OtaLawRw/1996/1.html

First Nations Information Governance Centre. (2020). *A First Nations data governance strategy*. https://fnigc.ca/news/introducing-a-first-nations-data-governance-strategy/

Gomberg, M. (2023). *Privacy laws, ethics and the conundrum of DNA*. IAPP News. https://iapp.org/news/a/privacy-laws-ethics-and-the-conundrum-of-dna-2

Government Chief Privacy Officer. (2024). *GCPO Guidance. How to create an information sharing agreement*. https://www.digital.govt.nz/assets/Standards-guidance/Privacy/How-to-create-an-Information-Sharing-Agreement-v1.0.pdf

Harmsworth, G. & Awatere, S. (2013). Indigenous Māori knowledge and perspectives of ecosystems. In J. R. Dymond (Ed.), *Ecosystem services in New Zealand – conditions and trends* (pp. 274 – 286). Manaaki Whenua Press.

Jackson, M. (2000). Where does sovereignty lie? In C. James (Ed.), *Building the constitution* (pp. 196-200). Institute of Policy Studies.

Kukutai, T., Campbell-Kamariera, K., Mead, A., Mikaere, K., Moses, C., Whitehead, J. & Cormack, D. (2023). *Māori data governance model*. Te Kāhui Raraunga. Available at https://www.kahuiraraunga.io/maoridatagovernanceResearch/Maori_Data_Governance_Model.pdf

Kukutai, T., Cassim, S., Clark, V., Jones, N., Mika, J., Morar, R., Muru-Lanning, M., Pouwhare, R., Teague, V., Tuffery Huria, L., Watts, D., & Sterling, R. (2023). *Māori data sovereignty and privacy* (Tikanga in Technology discussion paper). Te Ngira Institute for Population Research. Available at https://www.waikato.ac.nz/assets/Uploads/Research/Research-institutes-centres-and-groups/Institutes/Te-Ngira-Institute-for-Population-Research/MDSov-and-Privacy_20March2023_v2.pdf

Kukutai, T., Clark, V., Jacob, R., Jones, N., Morar, R., Muru-Lanning, M., Tarapa-Dewes, E., Pouwhare, R., Teague, V., Tuffery Huria, L., Watts, D., & Sterling, R. (2025). *Māori Data Privacy Framework.* Te Ngira Institute for Population Research.

Kukutai, T., & Taylor, J. (Eds). 2016. *Indigenous data sovereignty: Toward an agenda.* ANU Press. https://press.anu.edu.au/publications/series/caepr/indigenous-data-sovereignty

Law Commission. (2001). *Māori custom and values in New Zealand* (Study paper 9). https://www.lawcom.govt.nz/assets/Publications/StudyPapers/NZLC-SP9.pdf

Law Commission. (2008). *Privacy concepts and issues: Review of the law of privacy, Stage 1* (Study paper 19). https://www.lawcom.govt.nz/assets/Publications/StudyPapers/NZLC-SP19.pdf

Law Commission (2010). *Review of the Privacy Act 1993. Review of the law of privacy. Stage 4* (Issues paper 17). https://www.lawcom.govt.nz/assets/Publications/IssuesPapers/NZLC-IP17.pdf

Law Commission. (2011). *Review of the Privacy Act 1993. Review of the law of privacy. Stage 4* (Report 123). https://www.lawcom.govt.nz/assets/Publications/Reports/NZLC-R123.pdf

Law Commission. (2020). *The use of DNA in criminal investigations* (Report 144). https://www.lawcom.govt.nz/assets/Publications/Reports/NZLC-R144.pdf

Law Commission. (2023). *He Poutama* (Study paper 24). https://www.lawcom.govt.nz/assets/Publications/StudyPapers/NZLC-SP24.pdf

Manheim, K., & Kaplan, L. (2019). Artificial intelligence: Risks to privacy and democracy. *Yale JL & Tech.*, *21*, 106.

Martin, K. & Zimmermann, J. (2024). Artificial intelligence and its implications for data privacy. *Current Opinion in Psychology, 58*. doi.org/10.1016/j.copsyc.2024.101829.

Mead, H. M. (2013). *Tikanga Māori: Living by Māori values*. Huia.

Mikaere, A. (2007). Tikanga as the first law of Aotearoa. *Yearbook of New Zealand Jurisprudence, 10,* 24–31.

Office of the High Commissioner for Human Rights. (2016). *Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci* (A/HRC/31/64). United Nations. https://www.ohchr.org/en/special-procedures/sr-privacy#:~:text=Privacy%20enables%20the%20enjoyment%20of,economic%2C%20social%20and%20cultural%20life

Office of the Ombudsman. (2020). *Privacy. A guide to section 9(2)(a) of the OIA and section 7(2)(a) of the LGOIMA*. https://www.ombudsman.parliament.nz/resources/privacy-guide-section-92a-oia-and-section-72a-lgoima

Office of the Privacy Commissioner. (2020). *Health Information Privacy Code 2020.* https://www.privacy.org.nz/assets/New-order/Privacy-Act-2020/Codes-of-practice/Health-information-privacy-code-2020/HIPC-Amendment-No-1/Consolidated-Code-incorporating-Amendment-No-1.pdf

Office of the Privacy Commissioner. (2023a). *A potential biometrics code of practice: Discussion document.* https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Guidance-resources/Biometrics/Biometrics-November-2023/Biometrics-discussion-document.pdf

Office of the Privacy Commissioner. (2023b). '*A potential biometrics code of practice: Discussion document' – Summary of submissions*. https://www.privacy.org.nz/assets/New-

order/Resources-/Publications/Guidance-resources/Biometrics/Biometrics-November-2023/Summary-of-submissions-on-OPC-discussion-document.pdf

Office of the Privacy Commissioner. (2024). *Research on privacy concerns and data sharing.* https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Surveys/2024-04-30-Privacy-Commission-Report-Mar-24-FINAL-A969809.pdf

Office of the Privacy Commissioner. (2025a). *Biometric Processing Privacy Code 2025.* https://www.privacy.org.nz/assets/Codes-of-Practice-2020/Biometrics/060825-Biometric-Processing-Privacy-Code-2025-A1102662.pdf

Office of the Privacy Commissioner. (2025b). *Biometric Processing Privacy Code – guide.* https://www.privacy.org.nz/assets/DOCUMENTS/Biometrics-Guidance/2025-Full-Biometrics-Guidance-October-2025-updates-post-publication-PDF.pdf

Office of the Privacy Commissioner. (2025c). *Inquiry into Foodstuffs North Island trial use of facial recognition technology.* https://www.privacy.org.nz/assets/DOCUMENTS/20250603-FRT-Inquiry-Report-A1082856.pdf

Office of the Privacy Commissioner and Independent Police Conduct Authority. (2022). *Joint inquiry by the Independent Police Conduct Authority and the Privacy Commissioner into Police conduct when photographing members of the public*. Office of the Privacy Commissioner. https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Commissioner-inquiries/8-SEPTEMBER-2022-IPCA-AND-OPC-Joint-Inquiry-into-Police-photographing-of-members-of-the-public.pdf

O'Shea, R. (2024, 31 October). Foodstuffs North Island's facial recognition trial: do the numbers add up? *Consumer*. https://www.consumer.org.nz/articles/foodstuffs-north-island-s-facial-recognition-trial-do-the-numbers-add-up

Paewai, P. (2024, 17 April). *Māori woman mistaken as thief by supermarket AI not surprising, experts say.* RNZ News. https://www.rnz.co.nz/news/national/514523/maori-woman-mistaken-as-thief-by-supermarket-ai-not-surprising-experts-say

Post, R. (2001). Three concepts of privacy. *The Georgetown Law Journal, 89*, 2087–2098. Available at https://openyls.law.yale.edu/server/api/core/bitstreams/075f2a6f-6acc-47de-b49d-26bff9b83701/content

Quince, K. (2016). Māori concepts in privacy. In S. Penk & R. Tobin (Eds.), *Privacy law in New Zealand* (2nd ed.) (pp. 29–52). Thomson Reuters.

Quince, K. & Houghton, J. (2023). Privacy and Māori Concepts'. In S. Penk & R. Tobin (Eds.), *Privacy Law in New Zealand* (3rd ed.) (pp. 43–136). Thomson Reuters.

Roberts, M. (2013). Ways of seeing: Whakapapa. *Sites: A Journal of Social Anthropology and Cultural Studies*, *10*(1), 93–120. https://doi.org/10.11157/sites-vol10iss1id236

Sluka, J. A. (2010). The Ruatoki Valley 'anti-terrorism' police raids: losing 'hearts and minds' in Te Urewera. *Sites: a journal of social anthropology and cultural studies*, *7*(1), 44-64.

Solove, D. (2002). Conceptualizing privacy. *California Law Review*, *90*, 1087–1155. Available at https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2086&context=faculty_publications

Tauri, J., & Deckert, A. (2022). Walking while brown: A critical commentary on the New Zealand Police extra-legal photographing and surveillance of rangatahi Māori. *Decolonization of Criminality and Justice, 4*(1), 69–75. https://doi.org/10.24135/dcj.v4i2.52

Te Kāhui Raraunga. (2021a). *Iwi data needs*. https://www.kahuiraraunga.io/iwidataneeds

Te Kāhui Raraunga. (2021b). *Māori data governance co-design outcomes report*. https://www.kahuiraraunga.io/maoridatagovernance

Te Mana Raraunga. (2018). *Principles of Māori data sovereignty.* https://www.temanararaunga.maori.nz/

Te Pou Matakana Limited v Attorney-General (No 1), NZHC 2942_ (high.court 2021). https://www.courtsofnz.govt.nz/assets/Uploads/2021-NZHC-2942.pdf

Te Pou Matakana Limited v Attorney-General (No 2), NZHC 3319_ (high.court 2021). https://www.courtsofnz.govt.nz/assets/cases/2021/2021-NZHC-3319.pdf

Tsosie, R. (2019). Tribal data governance and informational privacy: Constructing "Indigenous data sovereignty". *Montana Law Review*, *80*(2), 229–268. Available at https://scholarworks.umt.edu/mlr/vol80/iss2/4/

Waitangi Tribunal. (2021). *Report on the comprehensive and progressive Agreement for Trans-Pacific Partnership* (WAI 2522). Available at: https://forms.justice.govt.nz/search/Documents/WT/wt_DOC_178856069/CPTTP%20W.pdf

Walter, M., Kukutai, T., Carroll, S., & Rodriguez-Lonebear, D. (Eds.) (2020). *Indigenous data sovereignty and policy.* Routledge.

Warren. S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review 4*(5), 193–220. Available at https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

Williams, J. (2013). Lex Aotearoa: An heroic attempt to map the Maori dimension in modern New Zealand law – The Harkness Henry Lecture. *Waikato Law Review*, *21*, 1–34. http://www.nzlii.org/nz/journals/WkoLawRw/2013/2.html

New Zealand Legislation

Bill of Rights Act 1990. https://www.legislation.govt.nz/act/public/1990/0109/latest/DLM224792.html

Coroners Act 2006. https://www.legislation.govt.nz/act/public/2006/0038/latest/whole.html

Education and Training Act 2020. https://www.legislation.govt.nz/act/public/2020/0038/latest/LMS170676.html

Employment Relations Act 2000. https://www.legislation.govt.nz/act/public/2000/0024/208.0/DLM58317.html

Health (Cervical Screening (Kaitiaki)) Regulations 1995. https://www.legislation.govt.nz/regulation/public/1995/0029/latest/DLM198873.html

Official Information Act 1982. https://www.legislation.govt.nz/act/public/1982/0156/latest/DLM64785.html

Oranga Tamariki Act 1989. https://www.legislation.govt.nz/act/public/1989/0024/latest/DLM147088.html

Privacy Act 2020. https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23312.html?search=sw_096be8ed81f40d32_code_25_se&p=1

Resource Management Act 1991. https://www.legislation.govt.nz/act/public/1991/0069/latest/DLM230265.html

International Declarations and Guidelines

AI Principles. Organisation for Economic Cooperation and Development. (2024, first published 2019). https://www.oecd.org/en/topics/sub-issues/ai-principles.html

G20 AI Principles. Organisation for Economic Cooperation and Development. (2019, 9 June). https://oecd.ai/en/wonk/documents/g20-ai-principles

General Data Protection Regulation (*GDPR*) (EU Regulation 2016/679). The European Parliament and The Council Of The European Union. (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Guidelines for the Protection of Privacy and Transborder Flows of Personal Data. Organisation for Economic Cooperation and Development. (2013). https://legalinstruments.oecd.org/public/doc/114/114.en.pdf

International Covenant on Civil and Political Rights (ICCPR). United Nations Office of the High Commissioner for Human Rights. (1966). https://www.ohchr.org/sites/default/files/ccpr.pdf

Recommendation of the Council on Artificial Intelligence. Organisation for Economic Cooperation and Development. (2024, first published 2019). https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

Recommendation on the Ethics of Artificial Intelligence. United Nations Educational, Scientific and Cultural Organization (UNESCO). (2022). https://unesdoc.unesco.org/ark:/48223/pf0000381137

Report of the Special Rapporteur on the right to privacy (A/HRC/31/64, 24). United Nations General Assembly, Human Rights Council. (2016, 24 November). https://documents.un.org/doc/undoc/gen/g16/262/26/pdf/g1626226.pdf

The right to privacy in the digital age (A/HRC/RES/28/16). United Nations General Assembly, Human Rights Council. (2015, 1 April). https://docs.un.org/en/A/HRC/RES/28/16

United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP). United Nations. (2007). https://www.un.org/development/desa/indigenouspeoples/wp-content/uploads/sites/19/2018/11/UNDRIP_E_web.pdf

United Nations Convention on the Rights of the Child (UNCRC). United Nations. (1989). https://www.cypcs.org.uk/rights/uncrc/

Universal Declaration of Human Rights (UDHR). United Nations. (1948). https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf