Māori Data Sovereignty and Privacy

Tikanga in Technology Discussion Paper

March 2023

Te Ngira
Institute for
Population Research
THE UNIVERSITY OF WAIKATO

Authors

Tahu Kukutai, Shemana Cassim, Vanessa Clark, Nicholas Jones, Jason Mika, Rhianna Morar, Marama Muru-Lanning, Robert Pouwhare, Vanessa Teague, Lynell Tuffery Huria, David Watts & Rogena Sterling

To cite this publication

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. Hamilton: Te Ngira Institute for Population Research. https://doi.org/10.15663/j21.35481

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 Mere Kepa, Jesse Porter and the Office of the Privacy Commissioner. Kāore e ārikarika ngā mihi ki tō mātou Kāhui Kaumātua. Mei kore ake rātou hei ārahi i a mātou. Any errors or omissions are ours alone.

Definitions

algorithms

A series of steps through which particular inputs can be turned into outputs. An algorithmic system is a system that uses one or more algorithms to produce outputs that can be used for making decisions.

data controller

Usually the company, person or other body that has the power to decide what happens to the data in their possession. The Privacy Act 2020 uses the term ‘agency’ rather than ‘data controller’ and distinguishes between New Zealand and overseas agencies.

Māori data

Māori data refers to digital or digitisable information or knowledge that is for, from or about Māori and the places that Māori have connection with. Māori data is both qualitative and quantitative. It 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 in all its form including pūrākau, karakia, haka, waiata tawhito and pakiwaitara.

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.

public sector

The public sector includes the public service, state sector and local government.

Glossary

Aotearoa	New Zealand
āria	physical representation or resemblance of a person
ariki	supreme chief
atua	gods, influential ancestors
harakeke	flax native to Aotearoa, *phorium tenax*
haka	vigorous dance with actions and rhythmically shouted words
hapū	sub-tribe, clan
hau	spiritual breath of life
hongi	customary Māori greeting which involves pressing noses
iwi	tribe
kāhui kaumātua	council of elders
kawa	immutable protocols
kaitiaki	guardian
kaitiakitanga	guardianship, stewardship
karakia	traditional ritual chant done to acknowledge atua Māori or the environment
kawakawa	plant with a long history of medicinal use by Māori, *Piper excelsum*
kāwanatanga	the Crown's authority and control; government
koromiko	plant with a long history of medicinal use by Māori, *Veronica salicfolia*
kūmara	sweet potato
mana	spiritual authority, power, influence, status, prestige
mana motuhake	Māori self-determination, authority
manaakitanga	reciprocity
mātanga raraunga Māori	Māori data experts
mātauranga	Māori knowledge systems and ways of knowing
mauri	life force
mōteatea	lament or traditional song
noa	unrestricted, be free of tapu
pakiwaitara	narrative, legend
pātere	a chant
pūrākau	historic narratives (see te kura huna, te kura tūrama)
rāhui	prohibition or a ban
rangatahi	Māori youth
rangatira	chief
rangatiratanga	chieftainship

rongoā	traditional Māori medicine based on the transmission of intergenerational knowledge
taonga	those things and values that we treasure, both intangible and tangible
taonga katoa	all treasured things
tapu	sacred, restricted or prohibited
te ao Māori	the Māori world
te kura huna	esoteric and tacit knowledge
te kura tūrama	physical and evident knowledge
te reo Māori	the Māori language
te Tiriti o Waitangi	the Treaty of Waitangi
tinana	the physical self or body
tino rangatiratanga	Māori authority and control/ absolute control
takahi mana	trampled on
tikanga	values and practices for proper conduct
tinana	body
tuna	eel
tupuna	ancestor
tohi	consecratory rites
tohunga	an expert of their field of knowledge
urupā	burial grounds
utu	a concept to return to and maintain balance
waiata tawhito	ancient chants or compositions
wairua	spirit
waka	broad term is used for a variety of traditional water vehicles
wānanga	space for collective thinking and deliberation
whakapapa	genealogy; lineage
whānau	family
whanaungatanga	obligations
wharenui	traditional meeting house
whenua	land

Initialisms

CANZUS	Canada, Australia, (Aotearoa) New Zealand, United States
DIKW	Data-Information-Knowledge-Wisdom
DN	Digital Nations
FNIGC	First Nations Information Governance Centre
FPIC	free, prior and informed consent
FRT	facial recognition technology
GDPR	General Data Protection Regulation
HRA	Human Rights Act 1993
ICCPR	International Covenant on Civil and Political Rights
ICESR	International Covenant on Economic, Social and Cultural Rights
IDSov	Indigenous data sovereignty
IK	Indigenous knowledge
IP	intellectual property
IPPs	information privacy principles
IPRs	intellectual property rights
MBIE	Ministry of Business, Innovation and Employment
MDGov	Māori data governance
MDSov	Māori data sovereignty
OECD	Organization for Economic Cooperation and Development
OCAP™	Ownership, Control, Access and Possession (First Nations principles of governance)
PI	personal information
SRRP	(United Nations) Special Rapporteur on the right to privacy
TiNT	Tikanga in Technology research programme
TK	traditional knowledge
TMR	Te Mana Raraunga
TPM	Te Pou Matakana
UDHR	Universal Declaration of Human Rights
UNDRIP	United Nations Declaration on the Rights of Indigenous Peoples

Abstract

Privacy is a fundamental human right. One of its most important aspects is information privacy – providing individuals with control over the way in which their personal data is collected, used, disclosed and otherwise handled. Existing information privacy regulation neither recognises nor protects the collective privacy rights of Indigenous peoples. This paper explores Indigenous data privacy, and the challenges and opportunities, in the context of Aotearoa. It has two aims: to identify gaps in existing data privacy approaches with regards to Indigenous data, and to provide a foundation for progressing alternative privacy paradigms. We argue that while personal data protection is necessary, it is insufficient to meet the needs of Māori and Aotearoa more broadly. In so doing, we draw on three areas of research: Indigenous and Māori data sovereignty; data and information privacy, including collective privacy; and Māori and Indigenous privacy perspectives. We examine key features of the Aotearoa privacy context – including the Privacy Act 2020 (NZ) – and consider the implications of te Tiriti o Waitangi and tikanga Māori for alternative privacy approaches. Future options, including legal and extra-legal measures, are proposed.

Table of Contents

PART 1. INTRODUCTION

Purpose of this report

Data or information privacy, along with issues of trust and consent, are crucial to ethical data ecosystems (Calzada & Almirall, 2020; Geisler et al., 2021). Privacy is a fundamental human right and, in an increasingly 'datafied' world (van Dijck, 2014), information and data privacy laws, policies and standards are required to protect that right. In recent years a number of new data privacy laws have been developed and implemented to protect personal data rights, notably the European Union's General Data Protection Regulation (GDPR, 2016; see, Andrew & Baker (2021)) and, in Aotearoa New Zealand (Aotearoa hereafter), the Privacy Act 2020.

For Indigenous peoples, the protection of personal data is one part of a much wider set of data privacy considerations and Indigenous data rights (Global Indigenous Data Alliance, 2022). Indigenous data sovereignty (IDSov) refers to the inherent rights and interests that Indigenous peoples have in relation to the collection, ownership and application of Indigenous data (Carroll et al., 2019; Kukutai & Taylor, 2016; Walter et al., 2020). Indigenous data encompasses data, information and knowledge about Indigenous individuals, collectives, entities, lifeways, cultures, lands and resources (Rainie et al., 2019). While the term IDSov is relatively recent, the concept of having shared responsibilities for the protection and use of information and knowledge is an enduring one within Indigenous nations and communities. Any application of data privacy and protection to Indigenous data must thus address collective dimensions of privacy and be informed by values and concepts that are grounded in Indigenous knowledge systems and practices.

This paper explores the intersection of IDSov and data privacy, with a focus on Aotearoa. Its purpose is to both identify gaps in existing data privacy approaches with regards to Indigenous data and provide a foundation for alternative privacy paradigms. Such an exploration is timely. Māori data sovereignty (MDSov) and Māori data governance (MDGov) have become key considerations in the public sector as agencies seek to fulfil their Tiriti of Waitangi obligations, build their capacity and capability around Māori data for evidence-informed decision-making, and develop a more resilient and future-focused data ecosystem. The Māori Data Sovereignty Network Te Mana Raraunga (Te Mana Raraunga, 2017) and the Data Iwi Leaders group (Data ILG) of the National Iwi Chairs Forum have been at the forefront of efforts to give effect to MDSov (Kukutai et al., 2022). MDSov agreements have been signed between the Data ILG and government agencies committing to a significant work programme that meets iwi data priorities (Stats NZ, 2021). This includes the development of a Māori data governance model for use across the public service (Te Kāhui Raraunga

2021a, 2021b). However, despite the growing focus on MDSov and MDGov, relatively little attention has been paid to information privacy and the implications for Māori.

Privacy and privacy-related risks are not new but have become more complex, and far reaching, in the age of big and open data (see Appendix 1). Technologies now enable massive volumes of data to be collected, linked, analysed and shared in ways that were previously impossible. The digitisation of knowledge, the increasing interconnectedness of digital networks, as well as the promotion of open government data and open science, is shifting more Indigenous data into publicly accessible spaces. In many jurisdictions, legal and regulatory frameworks have failed to keep pace with technological and business developments in big data analysis. The practices of 'big tech' have raised numerous concerns about racial and gender bias in automated decision-making (Broussard, 2019; Eubanks, 2018; Noble, 2018; O'Neil, 2016), data colonialism (Couldry & Mejias, 2019) and surveillance capitalism (Zuboff, 2019). Data capitalism and data colonialism raise clear issues regarding privacy. Data colonialism combines the extractive practices of historical colonialism and extends the process of commodification into new spheres of social life, from work and education to health care, economic transactions, and familial and intimate relationships (Couldry & Mejias, 2019). For Indigenous peoples, this means a replay of their colonised experience as their data becomes open for exploitation and extraction of profit with little regard for their knowledge systems and concepts of protection and benefit (Cormack & Kukutai, 2022).

Legal developments in relation to Māori data have also highlighted the importance of research at the nexus of IDSov and privacy. The High Court's reasoning in the recent *Te Pou Matakana* cases (*No 1*, 2021; *No 2*, 2021) signalled that collective interests in data must be balanced against privacy interests, including individual privacy interests. The Court found that, in the context of the COVID-19 pandemic, the need to protect Māori lives by increasing vaccination rates outweighed privacy concerns relating to the disclosure of individuals' vaccination data. The decision was significant as it provides a strong basis for Māori to have access to Māori data held by the Crown. It also raises questions, which are largely unresolved, about the balance between individual and collective data rights, and the relationship between the protection of data and the protection of those from whom the data derive.

Concerns about data privacy have been heightened by recent data privacy breaches (e.g., the sharing of sensitive client data on Snapchat by Accident Compensation Corporation staff; see Bradley (2021)), data security breaches (e.g., the 2021 Waikato District Health Board ransomware attack), and an independent inquiry into police photographing of members of the public (Privacy Commissioner

and Independent Police Conduct Authority, 2022).[1] The expansion of facial recognition software across government agencies and the private sector with little to no public consultation, nor engagement with Māori, has also raised concerns.[2] Suffice to say there is no legal framework in Aotearoa that adequately recognises or protects Māori rights in relation to data.

Our starting point is that while personal data protection is necessary, it is insufficient to meet the needs of Māori in particular, and Aotearoa more broadly. Though personal privacy is still important to Indigenous peoples, it is collective privacy that cements Indigenous being, belonging and ways of life. Thus, a profoundly different approach is needed – one that balances collective as well as individual rights, upholds self-determination as a fundamental right, and is driven by values that are generative and restorative rather than extractive and punitive**.** While issues relating to personal data protection and privacy are well defined, individual data is now at "one end of a long spectrum of targets" in need of protection (Taylor et al., 2017b, p. 10). Despite growing recognition that group privacy cannot be reduced to the aggregate privacies of its members, research is sparse on how collective privacy should be defined, regulated and enacted. Moreover, there are few examples, anywhere, of collective or Indigenous privacy approaches guiding privacy law, policy and practice (Vis-Dunbar et al., 2011). This report, undertaken as part of the Tikanga in Technology (TiNT) research programme,[3] is a step towards addressing that gap.

Aotearoa is an ideal context within which to explore the intersection of IDSov and data privacy. Māori have complex kawa and tikanga around the protection and sharing of knowledge that safeguards information and maintains community cohesion. Kawa comprise edicts that are immutable and that serve to uphold the mana of iwi and hapū. Tikanga refers to 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; Stats NZ, 2020). Tikanga guide the way relationships are formed and the conduct of those relationships. In the context of privacy, tikanga guides the social relations between the private and public by attending to Māori principles of cultural operation (Law Commission, 2008, p. 104). We see much potential in tikanga-led approaches to privacy that can protect collective privacy, build trust and reduce group harm in diverse social, cultural and environmental settings.

[1] The inquiry was undertaken after complaints that police had stopped rangatahi in public places and photographed them without either their consent, or the consent of their parents or caregivers.

[2] https://www.rnz.co.nz/news/te-manu-korihi/471626/maori-data-specialists-not-consulted-on-facial-recognition-technology-data-sovereignty-expert

[3] https://tengira.waikato.ac.nz/research/tikanga-in-technology-indigenous-data-and-governance

There are also structural features of Aotearoa's data ecosystem that makes it a useful test ground for privacy innovation. Aotearoa is part of the DN group of the world's most digitally advanced nations.[4] The government has long had ambitious aspirations to be a "world leader in the trusted use of shared data" (New Zealand Data Futures Forum, 2015), and has enthusiastically adopted an explicit open-government approach (Open Data Charter, 2015; Stats NZ, 2021).[5] However, there are significant tensions between the open data movement and IDSov. As others have noted, the focus on increased data sharing among entities tends to gloss over the extraction and exploitation of Indigenous data by researchers, governments and corporations (Carroll et al., 2022; Hudson et al., 2020; Rainie et al., 2019), and ignore increasing demands by Indigenous peoples for greater control over the application and use of their data (Research Data Alliance Indigenous Data Sovereignty Interest Group, 2019).

This paper synthesises perspectives and evidence across three areas of research: Indigenous and Māori data sovereignty; data and information privacy; and Māori and Indigenous perspectives related to privacy. It also considers key features of the Aotearoa privacy context – including the Privacy Act 2020 (NZ) – and the implications of te Tiriti and tikanga for alternative privacy approaches. This report is not intended as a specialist legal report or a comprehensive review of the privacy literature. Rather, it aims to surface key concepts and issues and raise some critical questions that will need to be worked through to develop an approach to data privacy that is fit for Māori purposes. Our next step is to develop a Māori Data Privacy Framework, drawing on our review of the literature undertaken for this report, interviews with mātanga raraunga Māori, and wānanga undertaken with the TiNT kāhui kaumātua.[6]

We begin by defining key terms data, information and knowledge, but note that terminological and definitional issues beset the literature. These terms are used differently by different professions and experts, reflecting varying disciplinary perspectives. They also gain different shades of meaning when adapted to reflect the needs of information and communications technologies. Part 1 concludes with a brief background on personal and collective privacy, which sets out key approaches and definitions relevant to this paper.

[4] https://www.digital.govt.nz/digital-government/international-partnerships/digitalnations/

[5] The International Open Data Charter was approved by Cabinet in August 2017.

[6] https://tengira.waikato.ac.nz/research/tikanga-in-technology-indigenous-data-and-governance/tint-kaumatua-kahui

Data, information and knowledge

The distinction between data and information, and information and knowledge, is often vague. The words data and information are used interchangeably, and information and knowledge are often conflated. According to the *New Shorter Oxford English Dictionary*, *data*, in everyday usage, means:

1. things given or granted; things known or assumed as facts, and made the basis of reasoning or calculation
2. facts, especially numerical facts collected together for reference or information
3. the quantities, characters and symbols on which operations are performed by computers and other automatic equipment, and which may be stored and transmitted in the form of electrical signals, records on magnetic, optical or other mechanical storage media

(Brown, 1993).

Implicit in these definitions is the idea that data is the raw material that is used as the basis for proposing hypotheses, drawing conclusions and developing knowledge.[7] There are also definitions of data that refer to its subjective and symbolic features and functions (Zins, 2007).

It is difficult to separate data and information in any meaningful way. For example, the definition of data in the new Data and Statistics Act 2022 (NZ) also includes information, and the *New Shorter Oxford English Dictionary* defines *information* as:

> Knowledge or facts communicated about a particular subject, event, etc.; … Without necessary relation to a recipient: that which inheres in or is represented by a particular arrangement, sequence or set, that may be stored in, or transferred by, and responded to by inanimate things.
>
> (Brown, 1993)

Thus, information may consist of facts (data) but can also be knowledge or an assemblage of facts that are arranged or curated in a systematised way.

Knowledge has been defined as:

> a fluid mix of framed experience, values, contextual information, expert insight and grounded intuition that provides an environment and framework for evaluating and incorporating new experiences and information.
>
> (Davenport & Prusack, 1998)

[7] In keeping with general usage, we use the singular form of data throughout this report.

Implicit in this definition is the assumption that knowledge involves more than just knowing a fact, or an aggregation of facts. Rather, knowledge involves analysis, critical thought and know-how using a variety of intellectual, cultural and philosophical approaches. An oft-used way of distinguishing between these concepts is the Data-Information-Knowledge-Wisdom (DIKW) model. This hierarchical model conceptualises data as a basic input at the base, information at the next level, knowledge higher up still, and wisdom at the apex (Ackoff, 1989; for a critique of the DIKW hierarchy in relation to mātauranga Māori, see Mercier, Stevens & Toia, 2012).

When used in the context of Indigenous data, the term data often includes data, information and knowledge. Thus, Indigenous data have been defined as:

1. information and knowledge about the environment, lands, skies, resources, and non-humans with which they have relations
2. information about Indigenous persons such as administrative, census, health, social, commercial, and corporate, and
3. information and knowledge about Indigenous Peoples as collectives, including traditional and cultural information, oral histories, ancestral and clan knowledge, cultural sites, and stories, belongings.

(Carroll et al., 2020).

The Māori data sovereignty principles apply a similarly broad definition of Māori data as "digital or digitisable information or knowledge that is about or from Māori people, our language, culture, resources or environments" (Te Mana Raraunga, 2018). Te Kāhui Raraunga (2021c) not only defines Māori data as data that is by, for or about Māori, but also any data that Māori have a connection to.

For the purpose of this report we use the term data generally to also include information. When applied to Indigenous and Māori data, we use a broader concept of data to include information and knowledge, including Indigenous knowledge (Jahnke & Sentina, 2017), traditional knowledge and mātauranga (Mercier, Stevens & Toia, 2012).

Personal privacy

The term privacy has always been difficult to define and has become even more complex in the context of information privacy. Privacy is considered a cornerstone issue in relation to freedom and democracy. Although there is a vast literature on privacy, there is no universally agreed definition. As a concept, privacy is founded on Western cultural notions of a division between the public and private spheres of an individual's life. The public sphere is generally considered to be the parts of

one's life experienced in the open (e.g., in the community, politics, etc.). The private sphere has been defined as "the realm of life where one retreats to isolation or to one's family" (Solove & Schwartz, 2011, p. 40). The law protects some, but not all, of the private sphere. In many instances, privacy protection is anchored by human rights law. The following section summarises key privacy concepts and approaches, noting the opportunities and shortcomings in relation to the protection of Indigenous and Māori data.

PRIVACY AS A HUMAN RIGHT

A right to privacy is one of the fundamental rights conferred under both the *Universal Declaration of Human Rights* (UDHR) (United Nations General Assembly, 1948) and the *International Covenant on Civil and Political Rights* (ICCPR) (United Nations General Assembly, 1966a).

Article 12 of the UDHR states:

> 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 ICCPR states:

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.

There is no definition of privacy in either the UDHR or the ICCPR. This lack of a definition is problematic. As the UN Special Rapporteur on the right to privacy (SRRP) has stated:

> While the concept of privacy exists in all societies and cultures — and has done so throughout the history of humankind — there is no binding and universally accepted definition of such a notion … worldwide there exists a considerable legal framework that could be useful for the protection and promotion of privacy. The usefulness of that legal framework is, however, seriously handicapped by the lack of a universally agreed and accepted definition of privacy. Even if 193 nations were signed up to the principle of protecting privacy, it would mean very little unless there was a clear understanding of what they had agreed to protect.
>
> (Cannataci, 2016, p. 8)

Moreover, under international law, the right to privacy is not absolute. Rather, it can be subject to a number of exceptions, known as derogations. This is recognised in Article 4(1) of the ICCPR:

> In time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed, the States Parties to the present Covenant may take measures

> derogating from their obligations under the present Covenant to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with their other obligations under international law and do not involve discrimination solely on the ground of race, colour, sex, language, religion or social origin.

In addition, privacy rights can be attenuated provided they are not arbitrary (under both the UDHR and the ICCPR) and are not unlawful (ICCPR). Concepts of arbitrariness and unlawfulness are treated as questions of legality, necessity and proportionality:

> In keeping with those principles, States may only interfere with the right to privacy to the extent envisaged by the law and the relevant legislation must specify in detail the precise circumstances in which such interference may be permitted. Interference is unlawful and arbitrary not only when it is not provided for by law but also when a law or the particular interference is in conflict with the provisions, aims and objectives of the Covenant. A limitation can only be lawful and non-arbitrary if it serves a legitimate purpose … The limitation must be necessary for reaching that legitimate aim and in proportion to that aim and must be the least intrusive option available. Furthermore, any limitation to the right to privacy must not render the essence of the right meaningless.
>
> (United Nations High Commissioner for Human Rights, 2018, p. 4)

Although Aotearoa acceded to the UDHR in 1948 and to the ICCPR through becoming a signatory to it, this does not mean that these international law rights automatically become a part of Aotearoa's domestic law – they do not unless they are enacted into law by the legislature.

Privacy also extends to *informational self-determination* which is personal control over such matters as how to present one's self in society, including control over one's words, images, portraits, reputation, and, critically in the computer age, control over access to and use of personal information (Eberle, 2001).

PRIVACY AS A HUMAN RIGHT IN AOTEAROA'S DOMESTIC LAW

In Aotearoa, the legal framework that protects human rights consists of two pieces of legislation: the Bill of Rights Act 1990 (Bill of Rights) and the Human Rights Act 1993 (HRA). The rights conferred under the Bill of Rights are based on the ICCPR. The Bill protects a range of rights including freedom of expression, freedom of religious belief, and freedom of movement. It requires the government and anyone carrying out a public function to observe the human rights it protects. However, the right to

privacy is not explicitly included in the Bill of Rights.[8] It thus follows that the Bill of Rights does not provide a legal foundation for protecting IDSov – wholly or partly – through a general right to privacy.

The HRA focuses on protecting individuals from discrimination and establishes a framework for the oversight of these rights through the Human Rights Commission. Like the Bill of Rights, the HRA does not confer a right to privacy, nor does it protect IDSov.

PROTECTION OF PRIVACY IN THE LEGAL SYSTEM

Privacy laws are considered to cover a range of similar but distinct rights. Solove (2002, p. 1008) argues that privacy can be conceptualised in six different ways:

- a right to be let alone
- limited access to the self – the ability to shield oneself from unwanted access by others
- secrecy – concealment of certain matters from others
- control over personal information – the ability to exercise control over information about oneself
- personhood – protection of one's personality, individuality and dignity
- intimacy – control over, or limited access to one's intimate relationships or aspects of life.

The legal systems of most Western countries protect some or all of these rights to varying degrees. Developments in privacy scholarship have extended the way in which privacy can be conceptualised beyond Solove's taxonomy. One of the most important of these developments is to view privacy as a right that is closely related to human dignity and autonomy:

> Privacy can be considered as the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals.
>
> (United Nations High Commissioner for Human Rights, 2018, p. 2).

Privacy can also be seen as an enabling right that supports the enjoyment of other fundamental rights including self-determination. The UN SRRP has argued that:

> 24. .... it is the Special Rapporteur's contention that: (a) such a right to dignity and the free, unhindered development of one's personality should be considered to be universally applicable; and (b) that already recognized rights, such as those to

[8] Section 21 of the Bill provides for the right to be secure against unreasonable search or seizure which has been recognised as providing a partial right to privacy of personal information (Privacy Commissioner, 2018).

privacy, freedom of expression and freedom of access to information, constitute a triad of enabling rights that are best considered in the context of their usefulness in enabling a human being to develop freely his or her personality …

25. It will be seen that, in many cases, the debate on privacy cannot be meaningfully divorced from that on the value of autonomy or *self-determination* (emphasis added). The latter term is one that has been discussed at length and, when related to privacy and personality rights, it has since 1983 in Germany given rise to a constitutional right to "informational self-determination". The appeal and validity of this concept needs to be evaluated further in the context of a global discussion on how the right to privacy should be better understood in 2016; possibly, in the context of a discussion on the protection and promotion of the fundamental right to dignity and the free, unhindered development of one's personality.
26. The triad of enabling rights mentioned above — privacy, freedom of expression and freedom of access to information — existed before the advent of digital technologies, as did the right to dignity and the free, unhindered development of one's personality.

(Cannataci, 2016).

Privacy, considered against these requirements and objectives, has a number of shared objectives with IDSov, particularly in respect of providing Indigenous peoples with rights to self-determination and the preservation and ongoing development of their traditional customs and practices.

COMMON LAW PRIVACY RIGHTS

In Aotearoa, a common law right to privacy was confirmed by the Court of Appeal in *Hosking v Runting* in 2004. By majority, it decided that there is a common law right to privacy in Aotearoa. There are two fundamental elements for a successful claim for interference with privacy:

- the existence of facts in respect of which there is a reasonable expectation of privacy, and
- publicity given to those private facts that would be considered highly offensive to an objective reasonable person.

While legal elements such as 'reasonable expectation' and 'highly offensive to an objective reasonable person' will often be analysed from the perspectives and values of the dominant culture, recent cases in Aotearoa have opened the doorway for tikanga perspectives to also be taken into account.

INFORMATION PRIVACY

Information privacy laws, which are often called data protection laws in Europe, are the most common form of privacy legislation. Such laws focus on personal data protection through conferring on individuals a measure of control over how their personal information is collected, used, disclosed, transferred, stored, and secured or otherwise handled.

Most information privacy laws are based around a set of principles first developed by the Organisation for Economic Cooperation and Development (OECD) in 1980 known as the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD, 2013). The OECD Principles are designed to address two key public policy interests. The first is to promote the free flow of personal data. The second, anchored in human rights privacy protections, provides individuals with a measure of control over their personal data. This control extends across the whole of the information lifecycle from the initial collection of personal data, through its authorised use and disclosure, ensuring that it is correct, up to date, accurate and securely stored. The evolution of information privacy laws has broadly followed a path that has led to a principles-based approach derived from the OECD principles, where national legislation establishes a legal framework that enacts privacy principles and sets up the legal framework for their application, enforcement, complaint handling and oversight. The legal framework also accounts for other competing public policy interests that are considered to override or attenuate individual privacy rights. Examples of these, often referred to as "privacy exceptions", include law enforcement, national security and judicial proceedings.

The focus of the OECD principles is on personal rights. The rights they confer are individual rights to exercise some control over the way in which personal information is collected, used, disclosed or otherwise handled. Frequently, a greater level of protection is given to a variety of categories of personal information considered to be sensitive. Common examples include health information, sexual preference, and political and philosophical beliefs. It follows that the OECD principles do not cover, and were not designed to protect, collective rights. This is an important distinction when it comes to assessing the extent to which information privacy law is fit for the purpose of protecting or supporting Indigenous data rights. This key point is discussed later in this report.

PRIVACY ACT 2020

Aotearoa's information privacy legislation is the Privacy Act 2020,[9] which came into effect on 1 December 2020, replacing the Privacy Act 1993. The 2020 Act focuses specifically on the protection of *personal information* (PI), defined in section 7 as:

> personal information—
>
> (a) means information about an identifiable individual;[10] and
>
> (b) includes information relating to a death that is maintained by the Registrar-General under the Births, Deaths, Marriages, and Relationships Registration Act 1995 or any former Act (as defined in section 2 of the Births, Deaths, Marriages, and Relationships Registration Act 1995).

The Act applies to the public and private sectors in Aotearoa and obliges them to comply with 13 *information privacy principles* (IPPs) that relate to: the purpose for collection; the source of information – collection from the individual; what to tell the individual about collection; manner of collection; storage and security of information; providing people access to their information; correction of personal information; ensure accuracy before using information; limits on retention of personal information; use of personal information; disclosing personal information; disclosure outside Aotearoa; and unique identifiers (Privacy Act 2020, s. 22). The Act aligns with international law insofar as it gives 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" (subs. 3(a)). As Paulger notes, consent is not the primary or default basis for collecting, using and disclosing personal information under the IPPs. Rather, "the default basis for collecting PI under the IPPs is that collection of PI must be necessary for a lawful purpose connected with a function or an activity of the agency" (p. 2).

The lack of a Tiriti clause in the Act means there are few explicit avenues under which Māori might assert or express their specific rights and interests in privacy, and information privacy in particular. The only indirect reference to consider te ao Māori perspectives under the current legislation is through the requirement that the Privacy Commissioner "takes into account cultural perspectives on privacy" (Privacy Act 2020, s. 21c). Section 21(c) applies across all of the Commissioner's functions, duties and powers, including the way in which the Commissioner interprets the IPPs, and the way in which the Commissioner approaches their code-making powers. However, there has been limited discussion about what the application of section 21(c) to Māori data privacy protection might look

---

[9] https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html

[10] In the same section of the Act, an individual is defined as "a natural person, other than a deceased natural person". There is no definition of 'identifiable individual' but generally this means a person who can be reasonably identified, either directly or indirectly, were the information to be disclosed.

like. We return to the Act and the gaps and possible pathways for the protection of Māori data privacy later in this paper.

Group and collective privacy

Data privacy laws, standards and scholarship have largely focused on personal privacy. The concept of group privacy is not new but, until recently, has received little attention. However, developments in digital technologies have given rise to a new wave of privacy and ethical concerns, involving the collective dimension of data protection and group rights (Helm, 2016; Taylor et al., 2017a). Powerful analytics make it possible to collect and analyse large amounts of data in order to identify patterns in groups' behaviour, where the individual is often incidental to the analysis (Mantelero, 2017; Taylor et al., 2017a). Data gatherers create groups, shape the population they intend to investigate, and collect information about members. In many cases, individuals are not aware of these designations, or their consequences, which may have the potential to affect their opportunities and life chances (Mantelero, 2017). This underscores the need to move from narrow views of privacy and security toward a holistic view of situated and collective informational practice that is a matter not only of individual choice-making, but also of social and political responsibility (Dourish & Anderson, 2006).

GROUP PRIVACY

Group privacy refers to the privacy that people seek in their associations with others (Bloustein, 1977). Group privacy regards the protection of facts, acts or decisions that concern a group's internal affairs and its organisational autonomy. A group right to privacy tends to be recognised as an aggregate of individual privacies (Mantelero, 2017, p. 141). That is, group privacy is based on individual rights to privacy as part of the group. Groups may be defined or organised by an attribute of individuals in association with one another within a group, or by an attribute of the group itself (Bloustein, 1977; Mantelero, 2017). Groups tend to be fluid and dynamic entities with an endless number of sizes, compositions and natures (Taylor et al., 2017a). The notion of group privacy still relies on confidentiality, which – in this case – is more closely connected to the secrecy of the activity of the group than the secrecy of the information shared within the group by its members (Mantelero, 2017). This understanding still largely pivots on assumptions derived from the individual right to privacy. In exploring group privacy, and its relevance for Indigenous concepts of privacy, it is useful to distinguish between defined and undefined groups.

Defined Groups

Defined groups are groups with a shared background; for example, culture or other collective purpose (Bisaz, 2012; Bloustein, 1977). Groups can be linked by familial, association of similar interests or traits, or other connected interests. They know of other members of the group (often knowing them

personally) and are usually aware of the consequences of being associated together (Mantelero, 2017). These groups have rights granted based on association together such as the right to assemble. Defined groups that have been denied basic liberties, including Jewish, Roma and LGBT peoples and communities, have been a focus of the codification of international human rights (Taylor et al., 2017). Defined groups have a collective interest in how information describing the group is generated and used (Mittelstadt, 2017).

Undefined Groups

The important difference between defined and undefined groups is that the latter lack a shared background, purpose, sense of agency or group identity due to being externally crafted by third parties (Floridi, 2014; Mantelero, 2017; Mittelstadt, 2017). They are undefined in that individuals designated as part of a group do not know other members, and often are not aware that they have been so designated, or of the consequences. Undefined groups are constructed, often algorithmically, through the identification of common characteristics that may not be visibly apparent to members (Floridi, 2014; Mittelstadt, 2017). Individuals are linked according to perceived similarities (e.g., age, ethnicity, geographical location) and new behavioural identity tokens (Johnston, 2022), allowing for predictions and decisions to be taken at a group rather than individual level. These groupings may be short-term or long enough to answer a question posed by a data processor. Such groupings are not static nor uniform and may change over time with new labels applied, tweaked or removed as patterns are identified from new inputs.

Undefined groups do not have the same rights and duties as defined groups including a right to privacy (Mittelstadt, 2017). While privacy-, fairness- and discrimination-aware analytics techniques have gone some way to protect the interests of such groups, a group privacy right would demand that the scope of such techniques – along with legal privacy protections – be expanded beyond currently protected 'offline' classes (and proxies thereof) (Mittelstadt, 2017). Mittelstadt (2017) suggests that protections for undefined groups should focus on negative social, economic and cultural impacts.

COLLECTIVE PRIVACY

The main difference between group and collective privacy is that *collective privacy* has an autonomous dimension (Mantelero, 2017, p. 141). In short, collectives are entitled to protection and a measure of autonomy (Kammourieh et al., 2017). An example provided by Floridi (2014) is the right of self-determination, which is held by a nation or group as a whole – Indigenous peoples are an exemplar. Collective privacy derives from a collective's rights and interests in its own self-determination, sovereignty and control over information, rather than those of its individual members (Newman, 2004).

Collective privacy does not negate an individual or group interest in privacy but comes from different relationships, responsibilities and intentions. Confidentiality and control over personal information are far less important than issues relating to the risks of discrimination and the negative outcomes arising from the analysis of personal data (e.g., mass or social surveillance) that can affect how the collective is perceived and/or treated. Against this background, collective privacy can be described as the right to limit the potential harms to the group itself that can derive from invasive and discriminatory data processing. As Floridi (2014) points out, sometimes the only way to protect the individual is to protect the group to which the individual belongs.

CHALLENGES FOR GROUP AND COLLECTIVE PRIVACY

The protection of group and collective privacy raises a number of tricky questions and considerations which existing privacy protection paradigms largely fail to address. Individual consent, for example, is seen as the cornerstone of personal privacy. However, the size and extent of databases and data-processing activities makes it increasingly difficult (if not impossible) for an individual to be aware of every data-processing activity that might include their data, to assess how far the processing is done legitimately, and if not, to request the cessation of activities or seek legal intervention (Taylor et al., 2017a). These challenges are amplified for groups. If privacy is seen as identity constitutive, then privacy is connected to the integrity of information constituting one's identity, and the integrity of that identity is breached when data or information is added without consent (Floridi, 2014; Mittelstadt, 2017). If individuals are assigned to a group, without their knowledge or consent, and decisions are made based upon the group-level analysis that affects those so designated, to what extent might that constitute a breach of privacy and/or consent? Does the violation of privacy involve more than an aggregated interest of individuals, but rather a constitutive element of the group? (see van der Sloot, 2017). Such questions are rarely raised, let alone addressed, within dominant privacy approaches.

Complex analytics raises other sorts of challenges for existing conceptualisations of privacy. Traditional identifiers (e.g., name, address) are increasingly irrelevant in analytics to learn something about people. Individuals can be clustered according to behaviours, preferences and other characteristics without being identified in the traditional sense (Floridi, 2014; Mittelstadt, 2017; van der Sloot, 2017). Members of the group only need to be classified, rather than identified, in order to be effectively targeted. These digital collective identifiers "disrupt the long-established link between the individual, identity and privacy" (Mittelstadt, 2017, p. 476). This is particularly problematic for small populations subject to high levels of statistical surveillance, such as Indigenous peoples. Consequently, peoples from marginalised groups including racial minorities and lower socio-economic groups are more likely to be the target of profiling using big data, algorithms and predictive modelling – whether explicitly or indirectly (Browne, 2015; Eubanks, 2018; Noble, 2018; Mann &

Matzner, 2019; Sandvig et al., 2016). For example, studies of automated decision-making for loans and rentals have shown biases against Black Americans (Weber et al., 2020) and racial biases in facial recognition technologies (FRTs) are well documented (e.g., Najibi, 2020). There are also numerous examples of gender biases in algorithmic decision-making – Amazon, for example, scrapped an automated hiring program that learned to discriminate against women, particularly in technical roles (Wicks et al., 2021).

Algorithmic classification can be considered a privacy invasive practice, but one that is not adequately regulated, given the regulatory focus on identifiable individuals (Mittelstadt, 2017). For example, existing European privacy protections suggest that privacy cannot be violated without identifiability (European Commission, 2012). The capacity of individuals to manage data about themselves is assumed to end once identifiers linking them to the data (such as name and address) are removed in ways that can't be recovered (Mittelstadt, 2017). However, analytics routinely creates shared identifiers and patterns that are "functionally equivalent to identifiers" and can be used to group individuals (Mittelstadt, 2017, p. 479). Actions by members in a group can change the identity tokens, and these changes, and decisions based upon them, can affect all members of that group including members not yet observed by the analytics system (Mittelstadt, 2017). Yet, this notion of shared ownership of identity is largely ignored and not afforded comparable status under existing data protection law (Leese 2014; Mittelstadt, 2017; Taylor et al., 2017a).

The pervasive yet often unseen nature of data and digital surveillance also works against collective mobilisation and action – if groups do not know that their rights are being breached, they are unlikely to take action to preserve them. Taylor (2016) thus argues that new forms of legibility created through algorithmic tracking make people visible to control, but invisible in terms of agency and rights. Her study examining the ethical implications of tracking human mobility using data from mobile phones in African countries, showed that communities can be subjected to discrimination without knowing that their personal right to privacy has been violated. There have been some instances of collective privacy rights being brought before European courts; for example, the *Habitants D´Alsemberg, de Beersel, de Kraainem, d´Anvers et Evirons, de Grand et Environs v Belgium* and *Habitants de la Région des Fourons v Belgium.*[11] However, such cases are still rare, as are real-world examples of collective privacy regulation. The introduction of legislation in the European Union, which gives consumers in the EU the right to file class-actions lawsuits in cases of mass harm, may yet result in collective action against corporations, given the EU's stronger data-protection regime. As awareness

[11] These cases represented people from communes whose children were being denied education in the language of families and their community.

of collective data-driven harms increases, it seems reasonable to expect that so too will pressure to regulate and sanction those responsible.

PART 2. UNDRIP, TE TIRITI O WAITANGI AND PRIVACY

In seeking to develop a more expansive and fit-for-purpose concept of data privacy for Aotearoa, this section situates privacy in the wider context of the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP), te Tiriti o Waitangi, and tikanga Māori. The omission of all three of these enabling mechanisms in past and present privacy legislation in Aotearoa is discussed.

UNDRIP

The United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP) is a legally non-binding global human rights instrument that articulates the rights and interests of Indigenous peoples (United Nations General Assembly, 2007). Aotearoa – along with Australia, Canada and the United States – initially voted against the UNDRIP and was one of the last countries to become a signatory, in 2010. In recent years, the government has taken steps toward implementing the UNDRIP and is currently consulting on how to give effect to it and the recommendations set out in the report *He Puapua* (Charters et al., 2019).

The UNDRIP recognises that Indigenous peoples have individual and collective rights to enjoy human rights and fundamental freedoms as set out in the International Bill of Rights Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights (ICCPR), and the International Covenant on Economic, Social and Cultural Rights (ICESR) (United Nations General Assembly, 1966b). The UNDRIP also recognises rights that are specific to Indigenous peoples. Notably, Article 3 sets out the rights and interests that enable Indigenous self-determination and the ability to freely determine political status and pursue economic, social and cultural development.

UNDRIP does not have a specific article referring to privacy, but Indigenous customs are core to a privacy concept. Articles 11 and 12 state that, in order to govern, Indigenous peoples have rights to their traditions and customs, including the right to maintain, protect and develop the past, present and future manifestations of their cultures, and the individual and collective privacy involved. Article 13 provides a right to "revitalize, use, develop and transmit to future generations their histories, languages, oral traditions, philosophies, writing systems and literatures, and to designate and retain their own names for communities, places and persons." The application of these is also reflected in Article 35 whereby Indigenous communities "have the right to determine the responsibilities of individuals to their communities."

Within the UN system, the SRRP is mandated to promote and protect the right to privacy in a number of ways including reviewing government policies and laws, and helping to ensure that national procedures and laws are consistent with international human rights obligations. It is thus significant that the SRRP has endorsed IDSov in two reports relating to big data and open data (Cannataci, 2018b), and the protection and use of health-related data (Cannataci, 2019). The latter report recommends that States provide Indigenous data governance to Indigenous peoples within their territorial boundaries. It also supports the rights of Indigenous peoples to:

- exercise control of health-related data that relates to Indigenous peoples. This includes the creation, collection, access, analysis, interpretation, management, security, dissemination, use, reuse, infrastructure and all other data processing of health-related data relating to Indigenous peoples
- access and be consulted on health-related data of Indigenous peoples that is contextual and disaggregated (available and accessible at individual, community and First Nations levels), and
- health-related data that is protective and respects the individual and collective interests of Indigenous peoples and First Nations.

In so far as the report asserts Indigenous control over all aspects of the Indigenous data life cycle, it includes Indigenous determination of information privacy in regard to Indigenous data. The SRRP also recognises that IDSov is supported by Indigenous peoples' wider rights to self-determination and governance "over their land, resources and culture" as set out in the UNDRIP (Cannataci, 2018a, para. 73).

Te Tiriti o Waitangi

Te Tiriti o Waitangi is widely accepted as Aotearoa's constitutional document that establishes and guides the relationship between Māori and the Crown. Tiriti clauses are now so common in legislation that Te Arawhiti | The Office for Māori Crown Relations has developed a bespoke guide for policymakers on the use of Tiriti clauses (Te Arawhiti, 2022). The omission of te Tiriti from the Privacy Act 2020, and the lack of explicit consideration given to Māori concepts of privacy or tikanga Māori is at odds with the growing significance of group and collective data privacy concerns, prior scholarship identifying the shortcomings of the prevailing privacy approach, and the substantial corpus of Tiriti jurisprudence, some of which we discuss below.

TE TIRITI JURISPRUDENCE

Among recent legislation that includes a Tiriti clause is the Data and Statistics Act 2022,[12] which repealed the Statistics Act 1975. One of the purposes of the Act is to "recognise and respect the Crown's responsibility to give effect to te Tiriti o Waitangi/the Treaty of Waitangi by providing for the interests of Māori in" data, statistics and research (clause 3(e)). Clause 4 imposes specific duties on the Government Statistician (Statistician) relating to engagement with Māori and the consideration of Māori interests in standards for determining how census data is collected, and the criteria and requirements for the use of data for research. Defined provisions codifying specific duties owed by the Crown to Māori are becoming increasingly common in modern legislative drafting such as the Public Service Act 2020 and the Education and Training Act 2020.

Clause 14 of the Data and Statistics Act 2022 sets out the duties of the Statistician relating to te Tiriti. In particular, the Statistician must recognise the interests of Māori "in the collection of data, the production of statistics, and access to, and use of, data for research as tools for furthering the economic, social, cultural and environmental well-being of Māori (including iwi and hapū) and the way in which data is collected, managed, and used for the production of official statistics and for research" (Clause 14(a)). The Statistician must also "foster the capability and capacity of Māori to collect and use data for the production of statistics, access and use data under this Act for research, and engage with the Statistician under this Act" (Clause 14(c)). The capability and capacity of Statistics New Zealand to understand te Tiriti and engage with Māori must also be maintained by the Statistician (Clause 14(b)).

While these types of Tiriti clauses provide for some level of government commitment, they have been described by the Waitangi Tribunal as "not so much an elaboration as a reductionist effort at a Treaty clause" (Waitangi Tribunal, 2019, p. 77). This is due to the use of phrases such as 'recognition and respect' over stronger language (and commitments) such as 'give effect to', 'not act in a manner inconsistent with', and 'recognise and provide for'. "The latter examples place a positive obligation on the Crown to interpret the Act in a manner consistent with Treaty principles" (Waitangi Tribunal, 2019, p. 77). However, in *Trans-Tasman Resources v Taranaki-Whanganui Conservation Board*, the Supreme Court held that such clauses require a broad and generous interpretation. In addition, constraining the ability of the decision-maker to respect Tiriti obligations should not be ascribed unless the intention is clear (*Trans-Tasman Resources Ltd v Taranaki-Whanganui Conservation Board*, 2021, para. 151).

[12] https://www.legislation.govt.nz/act/public/2022/0039/latest/LMS418574.html

Clause 15 of the Data and Statistics Act 2022 codifies the following principles for engaging with Māori:

(a) must begin early and be meaningful;
(b) should include early discussion of the ways in which the Statistician and Māori can most effectively engage in the particular context;
(c) should include consideration of opportunities for Māori to partner with the Statistician in relation to activities that are the subject of the engagement.

In particular, the Statistician must engage with Māori:

- when preparing a multi-year data and statistical programme (clause 19)
- before determining the manner of taking, and the data to be collected in, a census (clause 35), and
- before setting standards that relate to, but are not limited to, the manner of collecting or managing data, and access and use of data for research and the publication of results and methodologies of the research (clauses 90 and 91).

Under clause 49(1)(c)(i), the Statistician must take into account the risk of harm to Māori in determining whether the proposed research is in the public interest. These clauses are not exhaustive, as a broad and generous interpretation is required, and as such represent the minimum standards required under the Crown's obligation to give effect to te Tiriti and its principles.

DATA AS A TAONGA

Māori data is often described as a taonga (Te Kāhui Raraunga, 2021c; Te Mana Raraunga, 2017). Article 2 of te Tiriti guarantees the protection of iwi and hapū tino rangatiratanga over their taonga katoa. 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).

The Tribunal has defined taonga in a number of its reports. In the *Allocation of Radio Frequencies Report* (WAI 26/150), the Tribunal described the promotion of te reo Māori as a taonga and recommended that supporting mechanisms, such as the electromagnetic spectrum in promoting te reo on the radio, should also be afforded the same protection (Waitangi Tribunal, 1999, p. 51). In its report into *Claims Concerning New Zealand Law and Policy Affecting Māori Culture and Identity* (WAI 262), the Tribunal defined taonga species as species over which whānau, hapū and/or iwi claim kaitiaki obligations whose basis, history and content are set out in mātauranga Māori (Waitangi Tribunal, 2011, p. 64). Evidence heard in this claim related to relationships developed over 40 generations for practical uses including food (such as kūmara and tuna or eels) and rongoā Māori (Waitangi Tribunal, 2011, p. 65). Such evidence related to the use, methodologies, life cycles and

characteristics of these species. These species are not simply resources, but are situated within a broader relational matrix sourced in mātauranga Māori.

The Tribunal also defined taonga works in two ways: 1) a creation of the pre-existing and distinctive body of knowledge, values and insights known as mātauranga Māori; and 2) a result of the effort and creativity of Māori, both in modern times and the distant past. Each taonga work has a kaitiaki – those whose connection through whakapapa creates an obligation to safeguard the taonga itself and the mātauranga that underlies it. Examples of taonga works include mōteatea, pātere, karakia, carving, weaving, painting, constructions such as waka or wharenui and other crafts, and dramatic and musical works (Waitangi Tribunal, 2011, p. 30).

In its report on *The Comprehensive and Progressive Agreement for Trans-Pacific Partnership* (WAI 2522), the Tribunal did not specify which kinds of data are taonga in their own right, but recognised that mātauranga Māori included Māori rights and interests in the digital domain and this placed "a heightened duty on the Crown to actively protect those rights and interests, particularly in a field that is subject to rapid change and evolution". It also recognised that "from a te ao Māori perspective, the way that the digital domain is governed and regulated has important potential implications for the integrity of the Māori knowledge system, which *is* a taonga" (Waitangi Tribunal, 2021, p. 53).

While the Tribunal did not state that all data is taonga, it is reasonable to expect that some kinds of data may require more specific kinds of active protection given their sensitivity or value, and the contexts in which they are used. The Crown's responsibilities with regard to active protection of Māori data include influencing the broader settings within which the private sector collects, stores, uses and shares Māori data.

Tikanga and privacy

Tikanga is central to understanding, protecting and implementing Māori data privacy. While there are no tikanga provisions in the Privacy Act 2020, there is wider recognition of tikanga as part of the Aotearoa legal system. The Tribunal has described two spheres of authority in Aotearoa: one of tino rangatiratanga and one of kāwanatanga (Waitangi Tribunal, 2014, p. 527), each characterised by unique legal traditions. Writing extrajudicially, Williams (2013) describes these as the first law (Māori legal traditions) and the second law (British legal traditions). The first law – tikanga – is primarily values-based and focused on whakapapa. The second law distinguishes relationships from culture as being contractual and proprietary in nature.

The meeting point of these distinct legal traditions may be achieved through various means, including:

- incorporating tikanga into legislation
- tikanga as an extrinsic aid to statutory interpretation
- tikanga as part of the values of the common law, and
- tikanga as its own source of law, either within state law or as its own independent legal system.

A recent High Court decision concluded that tikanga is a "free-standing" legal framework recognised by New Zealand law (*Ngāti Whātua Ōrākei Trust v Attorney-General*, 2022), made by and for iwi and hapū (*Ngāti Whātua Ōrākei Trust v Attorney-General*, 2022, para. 64), and which must not be seen in terms of the English law heritage of the New Zealand common law (*Ngāti Whātua Ōrākei Trust v Attorney-General*, 2022, para. 37). It is possible for tikanga to determine the outcome of a court's application of statute or common law or be the source of legal rights enforced by the courts (*Ngāti Whātua Ōrākei Trust v Attorney-General*, 2022, para. 33). This significant legal development will shift how legal frameworks are applied in the future, including how the law of Aotearoa balances data and privacy rights.

PRIOR CONCERNS ABOUT PRIVACY LEGISLATION AND TIKANGA

It is important to note that the shortcomings of privacy legislation in Aotearoa with regard to collective Māori privacy considerations and tikanga are not new, but were identified and described in reports dating back more than a decade. In a review of the Privacy Act 1993, the Law Commission argued that the individualistic focus of privacy law did not take account of the collective interests of Māori groups (Law Commission, 2008, p. 106). The Commission noted that, even where a person's identity was de-identifiable, there may still collective interests involved (Law Commission, 2008, p. 107). The issue of 'collective ownership' and 'collective privacy' incorporated the idea of a whānau or hapū 'owning' their collective information, including aggregated or statistical data. This enabled their rights to make decisions about that information, including how it was shared, aggregated and published. Such arguments tend to use the concepts of privacy and ownership interchangeably. The claim to collective control of aggregated data is clearly related to broader notions of collective Māori property rights in information (Law Commission, 2008). Several concerns were noted in relation to privacy from a tikanga perspective:

- tensions existed between individual-focused Western concepts of privacy and Māori concerns with collective interests;
- issues of trust and concerns by Māori that their information may be used in ways that are disempowering or derogatory, or that diminish mana;

- questions about the collection of personal information for iwi and hapū registers, and about governance of personal information held by tribal authorities; and
- concerns about control over online information about Māori, including whakapapa information.

(Law Commission, 2011, p. 298)

The review gave a number of illustrative examples. One related to the treatment of deceased relatives. Under the Privacy Act 1993, section 2(1) defined *personal information* as "information about an identifiable individual" and *individual* as "a natural person, other than a deceased person". Not protecting a deceased person has implications for their living relatives, and the wider hapū and iwi. From a tikanga perspective, information relating to the deceased would still be considered private (Law Commission, 2008, p. 106). Under the current Privacy Act (s. 7(1)), an individual means "a natural person, other than a deceased natural person". Despite this definition, the Act does allow for a code of practice that applies one or more of the IPPs to information about deceased persons (s. 32(6)(a)).

Another example regarded the lack of protection afforded to whakapapa information. The Commission noted that such information is often considered tapu and protected by custodians on behalf of their whānau, hapū or iwi (Law Commission, 2008, p. 106). However, when such information is made accessible online, collective issues of privacy arise. One example involved making Māori land records open access. Placing them online enabled people to retrace their whakapapa and their rights and interests in land, but also limited the ability to have collective kaitiakitanga over such information (Law Commission, 2008, p. 106). Another example was making whakapapa information available online through genealogy sites or other specialist websites. Though such sites enabled individuals and whānau to connect to each other, and their wider hapū and iwi, it was also a clear violation of tapu, breaching protocols surrounding the transmission of knowledge, and placing information at risk of misuse by people seeking to claim rights based on fabricated whakapapa connections (Law Commission, 2008, pp. 106–107). It also enabled companies to profit from collectively owned information that they did not own, at least from a cultural rights perspective.

With regard to the place of tikanga informing privacy practices, the Commission noted that much of Māori public business is conducted on the marae, which is public to those of the marae but not to outsiders. Moreover, there is specific tikanga at each marae as to how information is shared both within and outside of the marae (Law Commission, 2008, p. 105). The review made a number of suggestions to ensure Māori needs and perspectives were addressed in the Act or any improvements to it:

- the development of guidance material dealing with issues that raise particular concerns for Māori
- the establishment by the Office of the Privacy Commissioner of an advisory group on issues of concern to Māori, and
- the development of a code of practice for the regulation of the handling of personal information in connection with iwi registers.

The review also found that while the Privacy Act 1993 was a flexible piece of legislation able to accommodate different cultural views about the nature and value of personal information and the desire to share, or limit the sharing, of personal information within group, the Act still, at its core, focused on individual rights and was thus difficult to apply within a collective context (Law Commission, 2011, p. 298). For that reason, any application of Māori privacy would require special provisions in legislation. Some issues might also be resolved through other legal means such as the development of Indigenous intellectual property rights, or special legal mechanisms to protect certain types of sensitive information relating to Māori or other groups.

THE SIGNIFICANCE OF TE POU MATAKANA CASE

More recently, the decisions from *Te Pou Matakana* show that a specific Tiriti clause is not required for the courts to consider te Tiriti, its principles and tikanga Māori as a relevant consideration when deciding whether to disclose information about Māori individuals.

TPM (trading as the Whānau Ora Commissioning Agency) was successful in its judicial review applications to the High Court challenging the Ministry of Health's decision not to provide them with the individual data of Māori in the North Island who had received any dose, or only one dose, of the COVID-19 vaccine (*Te Pou Matakana Limited v Attorney-General (No 1)*, 2021, para. 135; *Te Pou Matakana Limited v Attorney-General (No 2)*, 2021, para. 151). TPM argued that it needed the data for the successful implementation of its programme to boost Māori vaccination rates and prevent significant loss of life. The data consisted of personal details, contact details, vaccination status and vaccination booking status (*Te Pou Matakana Limited v Attorney-General (No 2)*, 2021, para. 1).

The High Court set aside the Ministry's first decision not to disclose the data, and the Director-General of Health accepted the recommendation from the Ministry not to disclose the data due to privacy concerns (the second decision) (*Te Pou Matakana Limited v Attorney-General (No 2)*, 2021, para. 3). The Ministry released the requested information to TPM shortly after the second decision was set aside by the High Court. However, the release was subject to certain conditions, such as the requirements for TPM to securely delete the information by the end of June 2022. The key issue was whether disclosure was necessary to prevent or lessen the serious threat to public health, and the

Ministry did not consider disclosure of individual data as appropriate or necessary to lessen the threat presented by COVID-19.

Although the Privacy Act 2020 is silent on te Tiriti and its principles, the High Court held the Ministry's power to disclose information under the Act must be exercised in accordance with te Tiriti and its principles (*Te Pou Matakana Limited v Attorney-General (No 1)*, 2021, para. 112). The Ministry had specifically committed to upholding and honouring the following obligations towards Māori in the vaccination programme (*Te Pou Matakana Limited v Attorney-General (No 1)*, 2021, paras 112–113):

- partnership
- tino rangatiratanga
- options
- equity, and
- active protection.

The Court ultimately found the Ministry did not have adequate regard to te Tiriti and its principles, as informed by tikanga, when it determined TPM's request for data (*Te Pou Matakana Limited v Attorney-General (No 1)*, 2021, paras 130–133).

Despite referring to the above obligations, the Ministry did not undertake any assessment of those principles in relation to TPM's particular request (*Te Pou Matakana Limited v Attorney-General (No 1)*, 2021, para. 131). This shows that, where Tiriti principles are engaged, there must be some evidence of decision-makers taking into consideration:

- the nature of these obligations (what do they require of the decision-maker)
- what they actually mean in the particular context (e.g., the vaccine rollout), and
- the ability of decision-makers to actually grapple with Māori interests (i.e., identify what interests are at play and how they inform the final decision).

This has significant implications for how the Court considered privacy concerns against the health and well-being of Māori, which was accepted as an increasingly vulnerable taonga at the time because of the 22.3 percentage point difference between the second vaccination coverage for Māori (58.1 per cent) and the rest of the population (80.4 per cent) (*Te Pou Matakana Limited v Attorney-General (No 2)*, 2021, para. 50).

The High Court accepted that, where taonga is at risk, not all tikanga principles, values or practices will be able to be perfectly fulfilled where they conflict with the central purpose of protecting the health and well-being of whakapapa (*Te Pou Matakana Limited v Attorney-General (No 2)*, 2021,

para. 109). The decision indicates that interests must be balanced so that privacy must be considered against the public health context. The urgency and importance of improving Māori vaccination rates potentially outweighed privacy concerns such that it was reasonable to disclose the individualised information if the public health outcome was more likely to be effective than the alternative of not disclosing individualised data.

The *Te Pou Matakana* decisions are important because they indicate that statements by the Crown that confirm a commitment to te Tiriti and its principles will create a legitimate expectation that the Crown must follow through with those commitments (*Te Pou Matakana Limited v Attorney-General (No 2)*, 2021, para. 120). Importantly, this does not require Tiriti obligations to be codified in statute. Both decisions support Māori (including Māori health providers and iwi) to request individualised data should it be necessary in particular circumstances.

The issue that was not addressed by the Court was the need for a tikanga-based framework for data sharing. Elsewhere, the Law Commission considered the place of Māori data in its report on *The Use of DNA in Criminal Investigations* (Law Commission, 2020). The Commission recognised that DNA holds special significance in te ao Māori as it contains whakapapa information, which is considered taonga, and its collection for use in criminal investigations gives rise to certain rights and responsibilities according to tikanga (Law Commission, 2020, para. 10). The Commission considered that for DNA legislation to be constitutionally sound, it should, at a minimum, provide a framework for Māori to articulate their rights and interests in the DNA regime and to participate in its oversight. In particular, new DNA legislation should recognise that tikanga may be engaged by various aspects of the regime and make provision for its operation, where appropriate (Law Commission, 2020, para. 12).

PART 3. INDIGENOUS AND MĀORI CONCEPTS OF PRIVACY AND PROTECTION

For centuries, tikanga served to protect, preserve and regulate access to information and knowledge within te ao Māori. Tikanga are fluid, flexible, custom-based and underpinned by fundamental values. While few studies have focused specifically on Indigenous or Māori concepts of privacy (Quince (2016) is an important exception), we draw on tikanga and mātauranga to describe what we see as core features of a Māori privacy approach. Whakapapa, mana, tapu, mauri and hau are particularly relevant, and are considered in turn.

Indigenous concepts of privacy

Though the notion of privacy may be considered a modern concept, most cultures and societies had principles that regulated interactions between the private and public spheres, and rules for when and how interference between these spheres was permitted (Herzfeld, 2009). The Western emphasis on the atomistic individual contrasts with other traditions that see humans as relational beings whose identity and reality turns on their relationships with others, their environs and, in some instances, what might be called the supernatural (Ess, 2008).

While there are few studies that directly examine Indigenous concepts of privacy, the wider literature from the CANZUS states (Anderson, 2017; Hudson et al., 2017; Gee, 2019; Victorian Information Commissioner, 2021; Vis-Dunbar et al., 2011; Williams et al., 2011) suggests a number of key features:[13]

- 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.

[13] Canada, Australia, (Aotearoa) New Zealand, United States

- Recognising and upholding relationships of belonging, responsibility and respect are paramount.

The First Nations OCAP™ principles (FNIGC, 2014) provide one example of Indigenous peoples enacting their own privacy laws and policies for personal and collective information (Schnarch, 2004, p. 13). The principles – which stand for Ownership, Control, Access and Possession – are not recognised in Canadian law, but nevertheless provide a means by which First Nations can work towards self-governance and protect collective privacy (FNIGC, 2020). As part of self-governance, having the ability to exercise jurisdiction builds capacity within communities for both personal and community privacy protection. FNIGC and OCAP™ principles challenge the assumption that if personally identifiable data has been removed, there are no longer privacy interests attached (FNIGC, 2014). FNIGC holds that, even where personal identifiers have been removed from data, collective privacy concerns remain and Indigenous rights and interests still pertain (FNIGC, 2014). For example, if data is considered sensitive from a cultural, commercial or privacy point of view, it should be restricted and not made publicly available. In these contexts, ownership of the data is a function of possession and control rather than any formal intellectual property right. While copyright can be used to legally restrict access to data sets and databases, data can be managed as a trade secret, or in a repository with restricted access.

Māori concepts of privacy

The Māori data sovereignty principles developed by the Māori data sovereignty network Te Mana Raraunga (2018) do not explicitly refer to privacy, but set out high-level values-based directives that are relevant to collective privacy considerations.

3.1 (Whanaungatanga|Obligations) Balancing rights. Individuals' rights (including privacy rights), risks and benefits in relation to data need to be balanced with those of the groups of which they are a part. In some contexts, collective Māori rights will prevail over those of individuals.

3.2 (Whanaungatanga|Obligations) Accountabilities. Individuals and organisations responsible for the creation, collection, analysis, management, access, security or dissemination of Māori data are accountable to the communities, groups and individuals from whom the data derive.

5.1 (Manaakitanga | Reciprocity) Respect. The collection, use and interpretation of data shall uphold the dignity of Māori communities, groups and individuals. Data analysis that stigmatises or blames Māori can result in collective and individual harm and should be actively avoided.

5.2 (Manaakitanga | Reciprocity). **Free, prior and informed consent** (FPIC) shall underpin the collection and use of all data from or about Māori. Less-defined types of consent shall be balanced by stronger governance arrangements.

6.2 (Kaitiakitanga | Guardianship). Ethics. Tikanga, kawa (protocols) and mātauranga (knowledge) shall underpin the protection, access and use of Māori data.

6.3 (Kaitiakitanga | Guardianship). Restrictions. Māori shall decide which Māori data shall be controlled (tapu) or open (noa) access**.**

In a seminal paper on Māori privacy, Quince (2016) explored how the disconnect between Western liberal notions of individualism and Māori collectivism produce very different cultural concepts of privacy, and how it is understood and applied. Despite there being no word for privacy in te reo Māori, there are well-defined tikanga that are central to a Māori concept of privacy, and that operate together to bring balance and order within human and non-human interaction and provide guidance when transgressed.

One obvious difference between Western and Māori concepts of privacy is the extent to which individuals are prioritised. The collective nature of Māori society emphasises communal identity and agency. Prior to colonisation, individuals largely existed in reference to their membership of broader collectives of whānau, hapū and iwi (Clark, 2017; Quince, 2016). The protection and advancement of group interests – rather than the individual – was paramount. In the 21st century, these rights and responsibilities are more complex and nuanced in te ao Māori, particularly in a digital context. Below we begin to explore how these different concepts can be operationalised in the contemporary context of data and data privacy.

WHAKAPAPA

Whakapapa is central to a concept of privacy within te ao Māori. Whakapapa is a genealogical layering and ordering that is a linear of descent-time and lateral of kinship-space (Kawharu, 2000, p. 349). It is the overarching framework of genealogy that demonstrates the relatedness between people, the natural world and the gods – the three spheres of the Māori universe (Marsden, 2003). Rights and obligations are understood through whakapapa and are thus relational rather than individually conferred. The tohunga Māori Marsden thus described the collective ethos within whānau and hapū:

> Because members were united on the basis of kinship ties the whānau or hapū group was regarded as an organism rather than an organisation. That is, that the group shared a corporate life and each individual [was] an integral member of that body or organism performing a particular function and role. Therefore, to serve

> others is to serve the corporate self. Thus loyalty, generosity, sharing, fulfilling one's obligations to the group, was to serve one's extended self.
>
> (Marsden, 2003, pp. 41–42).

Whakapapa has been central to the way Māori organised social and political units, from large groupings or iwi, to hapū and whānau (Mahuika, 2019). Interactions were guided by tikanga to ensure protections for both individuals and the collective in day-to-day life in what would generally be referred to as privacy today.

Whakapapa situates data in a relational context: all data comes from somewhere or someone. All individuals are part of a group – whether based on kinship, shared interests, attributes or status. Upholding whakapapa requires data privacy approaches that recognise and protect collective as well as personal privacy rights. Whakapapa also cautions against privileging data and data privacy protection at the expense of protecting actual whakapapa. Lady Tureiti Moxon addressed this in her evidence given in the TPM case, stating that: "There is taonga in life and health. If there is taonga in data, then that taonga must give way to life and health" (*Te Pou Matakana Limited v Attorney-General (No 2)*, 2021, para. 110).

TAPU

Tapu is an essential element of a Māori privacy concept. Tapu defines what is special and/or restricted, and can be applied to both animate and inanimate including humans, information and knowledge, objects and places (Benton et al., 2013; Mead, 2013). As Quince notes, "tapu provides us with the best analogy in tikanga to aspects of the Pākehā concept of privacy" (2016, p. 33).

In te ao Māori, personal privacy or tapu is underpinned by the value of human life and an individual's sanctity derived from that sense of worth (a normative inviolability of the person) that should not be breached by harmful action or words (Quince, 2016, p. 41). As a collective good, tapu covers places such as the home or the marae. While the collective concept of tapu is "circumscribed by ideas of privacy and exclusiveness", intrinsic tapu refers to the privacy notions of self-worth and respect due to all persons (Quince, 2016, pp. 41–42). As such, the tapu of the person is closely related to self-worth, dignity and essential humanity, and fully realised upon coming into existence (Benton et al., 2013; Mead, 2013; Quince, 2016).[14] Tapu is dependent upon the triad of tinana, wairua and mauri and exists by virtue of their descent from, and connection to, the atua, with those higher in the hierarchy

[14] Tapu is differentiated from mana which is "more malleable than tapu in the sense that it can wax and wane over a person's lifetime, according to their deeds, achievements and reputation. This is known as mana tangata – the mana of human existence, as apart from mana atua, power derived from whakapapa" (Quince, 2016, p. 35).

closer to the gods (Mead, 2013).[15] Included with the tapu of the person is the idea of 'personality'. In so far as a person retains a sense of self over his or her body, personality, possessions and mana,[16] he or she may be said to have privacy over these things (Quince, 2016, p. 32).

When information is tapu, there are limitations on how or with whom it should be shared (Henare, 2001; Mead, 2013). Knowledge essential to the group's survival was often held by tohunga as guardians of tikanga and mātauranga, and who had the mana to make decisions about its management and dissemination (Quince, 2016, p. 37). When applied to places, tapu marks places of significance (such as marae) or sacred places (such as urupā and battlegrounds) (Mead, 2013). Tikanga existed for each of these places. The ancient practice of rāhui – a temporary prohibition or a ban – is still routinely used as a protective mechanism to keep people and place safe. Examples include placing a temporary restriction, as a protective measure, over areas used for fishing, hunting or gathering (Mead, 2013; Quince, 2016), or where someone has died (e.g., in a river).

Quince (2016) states that in a legal sense, tapu relates to "the inviolability of the human person – to be free from physical assault and interference ... That sort of tapu is permanent, intrinsic and enduring, and is of spiritual (as opposed to human) origin" (p. 33). Rāhui is a different sort of tapu due to its temporary state but functions in a way similar to regulatory law in that it is reliant on human proclamation. In a digital context, one can see how the practice of rāhui might be applied to offer protection against invasive and harmful practices affecting individuals and groups. For example, in the context of facial recognition technologies, a rāhui might create space for Māori to determine the culturally appropriate treatment of FRT data including its classification, access, use and storage.

Noa – the state of being unrestricted – is a principle that acts in conjunction with tapu. When something becomes tapu, it requires certain actions to make it noa again. Noa conveys a sense of safety and openness – it is the profane, the secular, the everyday. However, tapu and noa are not fixed oppositional states but, rather, complementary parts of a dynamic system that enable the possibility of switching between the two (Anderson, 2017). The concepts of tapu, noa, mana and utu work together to maintain balance and order in society (Anderson, 2017; Mead, 2013).

[15] "The tinana is the physical self or body, the wairua the spiritual self/soul and mauri is the life force, divine spark or glue that binds these aspects together to provide the breath of life. Mauri is viewed as a reflection of one's physical, psychological and social health, so the desired norm is a mauri tau – a mauri at peace or balance, or mauri ora – a healthy life force" (Quince, 2016, pp. 34–35).

[16] Personality includes heirlooms and personal adornments. Individual property was valued for its connection to the mana of the owner, so private property was limited, but in spite of that still protected, and interference with another's personal items was deemed an affront to their mana, which may have required some form of utu (Quince, 2016, p. 36).

This all suggests that, in a digital context, it should be up to Māori to define whether Māori data is open or closed at any given time. De-identification practices should be sufficiently rigorous to offer protection for Māori individuals and groups, particularly given smaller population size combined with a higher probability of being part of a 'target' population of interest. The extension of tapu into data privacy also suggests that Māori should have the right to know whether their data is being used to develop and/or train machines or algorithms, and the right to opt out and to be digitally invisible. Data relating to mātauranga has special sensitivities that require active protection. As noted earlier in this paper, the Waitangi Tribunal has recognised that mātauranga is a taonga and that how "the digital domain is governed and regulated has important potential implications for the integrity of the Māori knowledge system". As the Law Commission noted in their review of earlier privacy legislation, active protection is particularly important for Māori data that is considered tapu, and that encodes information about related others, such as whakapapa and genetic data.

MANA

Mana refers to spiritual authority, power and ancestral efficacy (Henare, 2001, p. 208; Marsden, 2003). The concept of mana is "to be effectual, or to take effect" (Benton et al., 2013, p. 154). Along with tapu, mana is imbued from the gods at conception. The diminishing or violation of one's mana affects one's tapu or state of being. Thus, tapu and mana "need to be protected, strengthened and constantly confirmed so that balance, harmony, and potentialities can be fulfilled" (Henare, 2001, p. 208). Mana represents a person's (or thing's) reputation (it reflects our work, treatment of others, charisma and our moral character) and self-esteem – both how others think of me and how I think of myself (Quince, 2016, p. 34). When a person's mana has been violated, it indicates "takahi mana" – meaning that someone has trampled on your mana (Quince, 2016, p. 34).

To hold mana is to hold binding authority or power over one's domain including digital domains, whether individuals or group. This means that Māori should be the decision-makers over how Māori data is collected, stored, accessed, shared and used, including secondary uses. Holding mana over Māori data also means having a right to interrogate and influence data practices and processes that affect individuals and groups. In response to the question "Kei a wai te mana?" ("Who has the authority?"), a balanced approach to upholding individual and collective privacy is needed. The Māori data sovereignty principles note that in some contexts, collective Māori rights will prevail over those of the individual (Te Mana Raraunga, 2018).

MAURI

All things have mauri, which imbues it with its own specific character and force (Benton et al., 2013, p. 239; Henare, 2001). Henare (2001) defines mauri as:

> a concentration of life itself, like the center of an energy source and because of its power and energy, its purpose is to make it possible for everything to move and live in accordance with the conditions and limits of its existence.
>
> (p. 208)

Mauri can also be understood as a generative state and expresses the relationship between things. For example, the Waikato River is the tupuna of Waikato iwi and hapū. The mana and mauri of the river represents the mana and mauri of the iwi (Muru-Lanning, 2016). Waikato Māori understand that when the state of the Waikato River is altered, its mauri is weakened, and this has an adverse effect on local Māori well-being (Muru-Lanning, 2016). This understanding resonates with Benton et al.'s (2013) articulation of mauri as a force with physical, psychological and philosophical implications.

Mauri permeates everything, including pūrākau and knowledge in its contemporary manifestations. Pūrākau as a Māori methodological construct draws on two forms of knowledge: the first is esoteric and tacit in nature (te kura huna), the second is physical and evident (te kura tūrama). In the process of work and reflection, artistic research is accompanied by wairua and mauri.

All forms of data possess mauri and require nurturing, care and respect in order to maintain its vitality across the data life cycle. Because the mauri of all things is interrelated, this means that the mauri of data and the mauri of those connected to it are interdependent. Thus, Māori data should be cared for and used in ways that enhance Māori well-being. Privacy law and standards should recognise that Māori data are taonga and provide robust protections against the misuse of data.

HAU

Hau has been referred to as the 'spiritual breath of life' or the 'divine spirit' (Henare, 2001; Marsden, 2003). Hau is a cosmic power and an all-encompassing vital essence of health and vigour, embodied in all persons and things (Benton et al., 2013, p. 76; Henare, 2001, p. 211). Hau represents a state of well-being and balance, based on reciprocity and trust. It can be understood as the invisible remnants of a person (or their āria), which can track and trace where a person has been. Hau is imparted at conception and pervades the whole being throughout one's life, never departing, becoming an intrinsic element in the growth and development of a person (Henare, 2001). Hau is shaped, influenced, enhanced and can be diminished by others. It not only resides with individuals but also within the collective, including spiritual, natural and social ecosystems (Nicholson 2019, p. 149). Due to its interrelationship with different entities, hau emphasises connectivity and mutual reciprocity. This is what Henare refers to as the "ethic of generosity". In the act of exchanging hau during hongi, relational connectivity between individuals and community members, and their mutual obligations to each other, is invigorated and reinforced (Dawes et al., 2021).

There are two other functions and representations of hau. The first is the reference as personality and character and even a personal aura – an external quality rather than an in-dwelling one (Best, 1982, pp. 32, 50–51). Another is the intangibility of hau such as in the "hau of a speech" (Best, 1982, p. 51). Lastly, the maintenance of hau is core to the ethical, the good, the way of life.

In digital worlds, hau symbolises a state of balance based on a moral code of reciprocity. Data practices that uphold hau would protect and maintain human dignity, not just of individuals but also of groups. Privacy protection would extend to notions of equity and justice. Where data breaches harmed Māori, hau would require a range of options for redress, including tikanga options. Free, prior and informed consent would underpin the collection and use of all Māori data, including secondary use.

Part 4: FUTURE DIRECTIONS

Privacy is both a fundamental human right and a gateway right that reinforces other rights such as the right to non-discrimination and freedom of expression. Big data technologies and practices pose challenges and risks to individual and collective privacy, particularly for marginalised and over-surveilled groups. While data privacy research, standards and laws focus on the protection of individual data, personal data protection is part of a much wider set of data privacy considerations and Indigenous data rights.

For Māori and other Indigenous peoples, the right to privacy includes collective rights that cannot be reduced to the individual privacies of its members. New data privacy frameworks and approaches are needed that account for collective rights to privacy and uphold information self-determination in more holistic and meaningful ways. Just as important as confidentiality and control over personal information are the data harms that can arise to groups from the analysis of personal data.[17] Data harm can take many forms, from algorithmic profiling that targets vulnerable groups, to issues of bias and inaccuracy in facial recognition tools used by law enforcement, and online hate and extremism (Christchurch Call, n.d.). Existing research shows that digital collective identifiers disrupt the long-established link between the individual, and notions of identity and privacy. Moreover, people from marginalised groups are more likely to be the target of profiling using big data, algorithms and predictive modelling. It is already well documented that Māori are over-surveilled and subject to discriminatory data practices. Recognising and protecting collective privacy limits the potential harms to the group.

This paper has identified a number of privacy issues for Māori arising from the status quo. A key concern is that the Privacy Act 2020 does not explicitly provide for the protection of privacy from te ao Māori perspectives. More specifically, it:

- has an exclusive focus on personal information and personal privacy, thus excluding group/collective information and privacy
- does not explicitly recognise tikanga Māori or Māori concepts of privacy, and
- does not have a Tiriti clause.

[17] Data harms refers to the adverse effects caused by uses of data that damage or set back a person, group, entity or society's interests.

There are various ways in which Māori might engage with data privacy. One is a tikanga-led approach that is more holistic than existing data privacy paradigms and that addresses the wider relationships between data and the people and places that it connects to. This might still address many of the same sensitivities that existing privacy approaches seek to address but do so using different conceptual tools and approaches.[18] As the recent Ngāti Whātua Trust case showed, tikanga is a "free-standing" legal framework recognised by New Zealand law, made by and for iwi and hapū, and must not be seen in terms of the English law heritage of New Zealand common law. When it comes to data privacy and protection, tikanga offers the foundations for an alternative legal paradigm that actively protects Māori data as a taonga.

There is also the question of how Māori engage with and influence privacy as it is currently articulated in regulations, policies, scholarship and wider societal expectations. The lack of a culturally responsive framework or guidelines for the application of existing privacy laws and standards to Māori data is an obvious gap requiring attention.

The Office of the Privacy Commissioner, as Aotearoa's privacy regulator, has a key role to play. As a Crown entity, the Commissioner is required to comply with Tiriti obligations,[19] even without a Tiriti clause in the Act. However, waiting for this requirement to be tested does not sit well with the principle of active protection. Amending the Act to include a Tiriti clause would clarify the specific expectations of the Crown in relation to privacy. This would be more desirable than leaving it for the Crown to decide the terms on which it will consider te Tiriti and tikanga until such time as those expectations are clarified (or imposed) by the courts as a result of litigation.

Issues and questions to consider

As the government seeks to give meaningful effect to MDSov through policies and practices, this will necessarily require rethinking privacy approaches to address collective privacy considerations. Below we set out some questions, aligned with the three parts of this paper, that we hope will stimulate further consideration of Māori data privacy approaches:

Collective and group privacy

- What is collective data?

[18] We thank Jesse Porter for his feedback here.

[19] The Office of the Privacy Commissioner is not bound by the Public Service Act (and s. 14 requiring agencies to support the Crown in its relationships with Māori under te Tiriti), but is part of the Crown and as such has obligations under te Tiriti, reinforced in the *Enduring Letter of Expectations for Statutory Crown Entities, 2019.* We also consider that the courts would infer an obligation to comply with te Tiriti given the constitutional significance of te Tiriti and tikanga Māori in Aotearoa's legal system.

- When does a collection of data about individuals become collective data about a group?
- How should consent be sought or given for uses of collective data?
- What might constitute an identifiable collective?
- Should all identifiable collectives have the same collective right to privacy?
- In what contexts does collective privacy matter most?
- How can collective privacy be protected?
- What are the possible tensions between individual and collective data privacy?
- What principles might be useful for balancing individual and collective data privacy rights?

Te Tiriti and tikanga

- What implications does te Tiriti have for privacy regulation, including legislation, standards, principles and directives?
- How might a Tiriti right to collective privacy be operationalised without an explicit Tiriti clause in the Privacy Act 2020?
- How can privacy regulations incorporate tikanga in meaningful ways?
- Should tikanga address the same sensitivities that privacy legislation seeks to address?
- How can tikanga guide a relational way of thinking about data and data privacy (i.e., if data is 'our relations')?
- What are the potential benefits and risks of incorporating tikanga into privacy regulations?
- How might tikanga address challenges that might arise with regards to individual and collective privacy?

Indigenous and Māori concepts of data protection

- How relevant and meaningful is the concept of privacy in te ao Māori?
- What kinds of Māori data require special/extra forms of protection?
- What kinds of Māori collectives require special/extra forms of privacy protection?
- How useful is it to reframe Western concepts of privacy using Māori concepts such as mana, tapu, mauri and hau?
- What can we learn from other examples/models of Indigenous data privacy?

Charting a path forward

Given the limitations of prevailing data regulations for realising a substantive form of MDSov, we see an urgent need for sui generis legislation in Aotearoa that recognises MDSov, protects Māori data and mandates implementation with related monitoring, evaluation and compliance functions. Such legislation, which would be genuinely world-leading in terms of both Indigenous and data rights, would support Māori control over Māori data in a manner consistent with MDSov and informational self-determination.

Aside from information privacy law, there are other potential forms of protection that provide guidance about the legal and policy frameworks that might be used to support MDSov and informational self-determination. These frameworks include using existing intellectual property rights (IPR) to protect Indigenous knowledge (IK). It is important to recognise, however, that the progress in relation to the recognition of IK within the intellectual property (IP) framework has been slow. For example, the World Intellectual Property Organization has been negotiating text for the recognition and protection of traditional knowledge, traditional cultural expressions, and genetic resources since 2000 and an end to those negotiations is still not apparent.

There are also opportunities beyond changes to the Privacy Act. One is the development of a Māori information code or Māori data privacy code. Under the Act, the Commissioner has the power to issue a code of practice in relation to the IPPs that become part of the law.[20] Codes modify the operation of the Act and set rules for specific industries, organisations or types of personal information. A code can also apply one or more of the IPPs to information about deceased persons – one might reasonably expect that information about deceased persons includes whakapapa information which, as earlier noted, has a clear collective dimension.

In developing a Māori information or Māori data privacy code (akin to, say, the Health Information Privacy Code 2020),[21] there are a number of challenges. A key one is that the Act only pertains to personal information about identifiable individuals – as such, the informational privacy of groups and collective data would seem to be out of scope of a code, even if constructed through the use of personal information about identifiable individuals. Nevertheless, the range of data privacy issues and concerns being raised by Māori, and the government's obligations to actively protect Māori data as a taonga, provide a basis for exploring this option further.

As the Law Commission noted more than a decade ago, there is still a need for culturally appropriate privacy guidance and frameworks. One option is the development and testing of a Māori data privacy framework that is tikanga-centred, and accounts for both personal and collective dimensions of privacy. Work on this is already well underway by the authors, with whakapapa, mana, tapu, mauri and hau identified as core concepts. These are protections that are intrinsic to how tikanga may apply in a legal sense when balancing access to data and privacy principles. A diverse range of use cases have also been selected for testing the framework and its practical application.

[20] 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, and/or (ii) exempting any action from an IPP, either unconditionally or conditionally; (b) apply 1 or more of the IPPs without modification; and (c) prescribe how 1 or more of the IPPs are to be applied or complied with.

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

Finally, we see opportunities for direct investment in Māori infrastructure to develop, test and implement a 'by Māori, for Māori' privacy proof of concept. Such an approach has already been proposed in relation to a Māori cloud service (Kukutai et al., 2022) and, in the future, could be readily applied to Māori informational privacy and protection.

References

Ackoff, R. L. (1989). From data to wisdom. *Journal of Applied Systems Analysis, 16*, 3–9.

Anderson, T. (2017). *Tū te tapu, tā te tapu: How can tikanga inform the use of big data*. Health Research Council of New Zealand.

Andrew, J., & Baker, M. (2021). The General Data Protection Regulation in the age of surveillance capitalism. *Journal of Business Ethics, 168*, 565–578. https://doi.org/10.1007/s10551-019-04239-z

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.

Best, E. (1982). *Māori religion and mythology: being an account of the cosmogony, anthropogeny, religious beliefs and rites, magic and folk lore of the Maori folk of New Zealand.* Part 2. Government Printer.

Bisaz, C. (2012). *The concept of group rights in international law: Groups as contested right-holders, subjects and legal persons*. Nijhoff.

Bloustein, E. J. (1977). Group privacy: The right to huddle. *Rutgers Camden Law Journal*, *8*(2), 219–283. Available from: https://heinonline.org/HOL/LandingPage?handle=hein.journals/rutlj8&div=24&id=&page=

Bradley, A. (2021, October 27). ACC staff caught posting private details of clients to Snapchat group. *Stuff*. Available from: https://www.stuff.co.nz/national/300439012/acc-staff-caught-posting-private-details-of-clients-to-snapchat-group

Broussard, M. (2019) *Artificial unintelligence: How computers misunderstand the world*. MIT Press.

Brown, L. (Ed.) (2019). *The new shorter Oxford English dictionary*. Oxford University Press.

Browne, S. (2015). *Dark matters*. Duke University Press.

Calzada, I., & Almirall, E. (2020). Data ecosystems for protecting European citizens' digital rights. *Transforming Government: People, Process and Policy*, *14*(2), 133–147. https://doi.org/10.1108/TG-03-2020-0047

Cannataci, J. (2016). *Report of the Special Rapporteur on the right to privacy* (A/HRC/31/64, United Nations General Assembly). Available from: https://undocs.org/A/HRC/31/64

Cannataci, J. (2018a). *Right to privacy* (A/73/438, United Nations General Assembly). Available from: https://undocs.org/A/73/438

Cannataci, J. (2018b). *Big data and open data taskforce report* (A/73/438, United Nations General Assembly). Available from: https://www.ohchr.org/en/calls-for-input/reports/2018/report-big-data-and-open-data

Cannataci, J. (2019). *Report on the protection and use of health-related data* (A/74/277, United Nations General Assembly). Available from: https://www.ohchr.org/en/calls-for-input/reports/2019/report-thee-protection-and-use-health-related-data

Carroll, S., Rodriguez-Lonebear, D., & Martinez, A. (2019). Indigenous data governance: Strategies from the United States Native nations. *Science Journal, 18*(31), 1–15. http://dx.doi.org/10.5334/dsj-2019-031

Carroll, S., Garba, I., Figueroa-Rodríguez, O. L., Holbrook, J., Lovett, R., Materechera, S., Parsons, 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 Journal, 19*(43), 1–12. http://doi.org/10.5334/dsj-2020-043

Carroll, S., Garba, I., Plevel, R., Small-Rodriguez, D., Hiratsuka, V. Y., Hudson, M., & Garrison, N. A. (2022). Using Indigenous standards to implement the CARE principles: Setting

expectations through tribal research codes. *Frontiers in Genetics, 13,* article 823309. https://doi.org/10.3389/fgene.2022.823309

Charters, C., Kingdon-Bebb, K., Olsen, T., Ormsby, W., Owen, E., Pryor, J., Ruru, J., Solomon, N., & Williams, G. (2019). *He puapua. Report of the Working Group on a plan to realise the UN Declaration on the Rights of Indigenous Peoples in Aotearoa/New Zealand*. Available from: https://www.nzcpr.com/wp-content/uploads/2021/04/He-Puapua.pdf

Christchurch Call (n.d.).*The Christchurch call to action to eliminate terrorist and violent extremist content online* Available from: https://www.christchurchcall.com/assets/Documents/Christchurch-Call-full-text-English.pdf

Clark, N. (2017, December 12). Using the Privacy Act for Māori. *Privacy Commissioner.* Available from: https://www.privacy.org.nz/blog/using-the-privacy-act-for-maori/

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). Palgrave Macmillan.

Couldry, N., & Mejias, U. (2019). *The costs of connection: How data are colonizing human life and appropriating it for capitalism.* Stanford University Press.

Crampton, J. W. (2015). Collect it all: National security, Big Data and governance. *GeoJournal, 80*(4), 519–531. https://doi.org/10.1007/s10708-014-9598-y

Culnane, C., Rubinstein, B.I. and Teague, V. (2017). Health data in an open world. arXiv preprint arXiv:1712.05627. https://arxiv.org/abs/1712.05627

Culnane, D., Rubinstein, A., Benjamin, I.P. and Teague, A. (2019). Stop the open data bus, we want to get off. arXiv preprint arXiv:1908.05004. https://arxiv.org/abs/1908.05004

Davenport, T., & Prusack, L. (1998). *Working knowledge: How organizations manage what they know*. Harvard Business School Press.

Dawes, T., Muru-Lanning, M., Lapsley, H., Hopa, N., Dixon, N., Moore, C., Tukiri, C., Jones, N., Muru-Lanning, M. & Oh, M. (2021). Hongi, harirū and hau: Kaumātua in the time of COVID-19. *Journal of the Royal Society of New Zealand, 51*(Supp. 1): S23–S36. https://doi.org/10.1080/03036758.2020.1853182

Dourish, P., & Anderson, K. (2006). Collective information practice: Exploring privacy and security as social and cultural phenomena. *Human–Computer Interaction, 21*(3), 319–342. https://doi.org/10.1207/s15327051hci2103_2

Durie, E. T. (1994). *Custom Law* [Research paper]. Victoria University of Wellington. Available from: https://www.wgtn.ac.nz/stout-centre/research-units/towru/publications/Custom-Law.pdf

Durie, M. (2001). *Mauri ora: The dynamics of Māori health*. Oxford University Press.

Eberle, E. (2001). The right to information self-determination. *Utah Law Review, 4,* 965-1016.

Ess, C. (2008). East–West perspectives on privacy, ethical pluralism and global information ethics. In H. Hrachovec & A. Pichler (Eds.), *Wittgenstein and the Philosophy of Information. Proceedings of the 30th International Ludwig Wittgenstein-Symposium in Kirchberg, 2007* (pp. 185–203). Ontos Verlag.

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.

European Commission. (2012). *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Available from: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52012PC0011

First Nations Information Governance Centre (FNIGC). (2014). *Ownership, control, access and possession (OCAP™): The path to First Nations information governance*. Available from: https://achh.ca/wp-content/uploads/2018/07/OCAP_FNIGC.pdf

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

Floridi, L. (2014). Open data, data protection, and group privacy. *Philosophy & Technology*, *27*, 1–3. https://doi.org/10.1007/s13347-014-0157-8

Garcia, D., Goel, M., Agrawal, A. K., & Kumaraguru, P. (2018). Collective aspects of privacy in the Twitter social network. *EPJ Data Science*, *7*(1), Article 1. https://doi.org/10.1140/epjds/s13688-018-0130-3

Garner, S. A., & Kim, J. (2018). The privacy risks of Direct-to-Consumer genetic testing: A case study of 23andMe and Ancestry. *Washington University Law Review*, *96*(6), 1219–1266.

Gee, K. (2019, August 22). I*ntroduction to Indigenous Canadian conceptions of privacy: A legal primer*. Available from: https://www.cba.org/Sections/Privacy-and-Access/Resources/Resources/2019/Runner-up-of-2019-Privacy-and-Access-Law-Student-E

General Data Protection Regulation (GDPR). (2016). *Official Journal of the European Union*, *2016*(679), 1–88. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Geisler, S., Maria-Esther, V., Cinzia, C., Farias, L., Avigdor, G., Jarke, M., Lenzerini, M., Missier, P., Otto, B., Paja, E., Pernici, B., & Rehof, J. (2021). Knowledge-driven data ecosystems toward data transparency. *ACM Journal of Data and Information Quality*, *14*(1), 1–12. https://doi.org/10.1145/3467022

Global Indigenous Data Alliance. (2022). *Indigenous Peoples' rights in data.* Available from: https://www.gida-global.org/new-page-1

Helm, P. (2016). Group privacy in times of big data. A literature review. *Digital Culture & Society*, *2*(2), 137–152. http://dx.doi.org/10.14361/dcs-2016-0209

Henare, M. (2001). Tapu, mana, mauri, hau, wairua: A Māori philosophy of vitalism and cosmos. In J. A. Grim (Ed.), *Indigenous traditions and ecology – The interbeing of cosmos and community* (pp. 198–221*)*. Harvard University Press.

Herzfeld, M. (2009). The performance of secrecy: Domesticity and privacy in public spaces. *Semiotica*, (175), 137–162. http://dx.doi.org/10.1515/semi.2009.044

Hosking v Runting, 1 NZCA 25 (Court of Appeal Court of Appeal 2004). Available from: https://www.5rb.com/wp-content/uploads/2013/10/Hosking-v-Runting-NZCA-25-Mar-2004.pdf

Hudson, M., Anderson, T., Dewes, T., Temara, P., Whaanga, H., & Roa, T. (2017). He matapihi ki te mana raraunga – Conceptualising big data through a Māori lens. n H. Whaanga, T. T. A. G. Keegan, & M. Apperley (Eds.), He Whare Hangarau Māori - Language, culture & technology (pp. 64–73). The University of Waikato.

Hudson, M., Garrison, N., Sterling, R., Caron, N. R., Fox, K., Yracheta, J., Anderson, J., Wilcox, P., Arbour, L., Brown, A., Taualii, M., Kukutai, T., Haring, R., Te Aika, B., Baynam, G. S., Dearden, P. K., Chagné, D., Malhi, R. S., Garba, I., … Carroll, S. R.. (2020). Rights, interests and expectations: Indigenous perspectives on unrestricted access to genomic data. *Nature Review Genetics*, *21*, 377–384. https://doi.org/10.1038/s41576-020-0228-x

Jahnke, T., & Sentina, M. (2017). *Indigenous knowledge: Issues for protection and management.* IP Australia, Commonwealth of Australia.

Johnston, A. (2022, February 2). Should birds of a feather be FloC'd together? *Salinger Privacy*. Available from: https://www.salingerprivacy.com.au/2022/02/02/floc/

Joly, Y., Dyke, S.O., Cheung, W.A., Rothstein, M.A. & Pastinen, T. (2015). Risk of re-identification of epigenetic methylation data: a more nuanced response is needed. *Clinical Epigenetics*, *7*(1), pp.1-3. https://doi.org/10.1186/s13148-015-0079-z

Kawharu, M. (2000). Kaitiakitanga: A Maori Anthropological Perspective of the Maori Socio-Environmental Ethic of Resource Management. *The Journal of the Polynesian Society*, *109*(4), 349–370.

Kuhlman, C., Jackson, L., & Chunara, R. (2020). No computation without representation: Avoiding data and algorithm biases through diversity. http://arxiv.org/abs/2002.11836

Kukutai, T., Clark, V., Culnane, C., & Teague, V. (2022). *Māori data sovereignty and offshoring Māori data.* Te Kāhui Raraunga. Available from: https://www.kahuiraraunga.io/_files/ugd/b8e45c_c035c550c8244c70a1025cd90a97298e.pdf

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

Kammourieh, L., Baar, T., Berens, J., Letouzé, E., Manske, J., Palmer, J., Sangokoya, D., & Vinck, P. (2017). Group privacy in the age of big data. In L. Taylor, L. Floridi, & B. van der Sloot (Eds.), *Group privacy: New challenges of data technologies* (pp. 37–66). Springer International Publishing.

Law Commission (2008). *Privacy concepts and issues: Review of the law of privacy, stage 1* (Study paper 9). Available from: https://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC%20SP19.pdf

Law Commission (2011). *Review of the Privacy Act: Review of the law of privacy, stage 4* (Report 123). Available from: https://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC%20R123.pdf

Law Commission (2020). *The use of DNA in criminal investigations* (Report 144). Available from: https://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/Law%20Commission%20-%20DNA%20in%20Criminal%20Investigations%20-%20Report%20144.pdf

Lee, C., & Zong, J. (2019, August 30). Consent Won't Magically Fix Our Data Privacy Problems. *Slate Magazine*. Available from: https://slate.com/technology/2019/08/consent-facial-recognition-data-privacy-technology.html

Leese, M. (2014). The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union. *Security Dialogue*, *45*(5), 494–511. https://doi.org/10.1177/0967010614544204

Mahuika, N. (2019). A brief history of whakapapa: Māori approaches to genealogy. *Genealogy*, *3*(2), 32. https://doi.org/10.3390/genealogy3020032

Mann, M., & Matzner, T. (2019). Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination. *Big Data & Society*, *6*(2). https://doi.org/10.1177/2053951719895805

Mantelero A. (2017). From group privacy to collective privacy: Towards a new dimension of privacy and data protection in the big data era. In L. Taylor, L. Floridi, & B. van der Sloot (Eds.), *Group privacy: New challenges of data technologies* (pp. 139–58). Springer.

Marsden, M. (2003). *The woven universe: Selected writings of Rev. Maori Marsden* (T. A. C. Royal, Ed.). Estate of Rev. Maori Marsden.

May, T. (2018). Sociogenetic risks - ancestry DNA testing, third-party identity, and protection of privacy. *New England Journal of Medicine*, *379*(5), 410-412. https://doi.org/10.1056/NEJMp1805870

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

Mercier, O. R., Stevens, N., & Toia, A. (2012). Mātauranga Māori and the data–information–knowledge–wisdom hierarchy: A conversation on interfacing knowledge systems. *MAI Journal, 1*(2), 103–106. https://www.journal.mai.ac.nz/sites/default/files/Pages%20103%20-%20116.pdf

Minister of Finance and Minister of State Services (2019). *Enduring Letter of Expectations for Statutory Crown Entities, 2019.* Available from: https://www.publicservice.govt.nz/assets/DirectoryFile/Enduring-Letter-of-Expectations-to-Statutory-Crown-Entities.pdf

Mittelstadt, B. (2017). From individual to group privacy in big data analytics. *Philosophy & Technology*, *30*(4), 475–494. https://doi.org/10.1007/s13347-017-0253-7

Muru-Lanning, M. (2016). *Tupuna Awa: People and politics of the Waikato River*. Auckland University Press.

Najibi, A. (2020, October 24). Racial discrimination in face recognition technology. *Science in the News*. Available from: https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/

Narayanan, A., Shi, E. and Rubinstein, B.I. (2011, July). Link prediction by de-anonymization: How we won the kaggle social network challenge. In The 2011 international joint conference on neural networks (pp. 1825-1834). IEEE.

Narayanan, A. and Shmatikov, V. (2008, May). Robust de-anonymization of large sparse datasets. In 2008 IEEE symposium on security and privacy (sp 2008) (pp. 111-125). IEEE.

Narayanan, A. and Shmatikov, V. (2019). Robust de-anonymization of large sparse datasets: a decade later. Available from: https://www.cs.princeton.edu/~arvindn/publications/de-anonymization-retrospective.pdf

Newman, D. G. (2004). Collective interests and collective rights. *The American Journal of Jurisprudence*, *49*(1), 127–163. https://doi.org/10.1093/ajj/49.1.127

New Zealand Data Futures Forum. (2015). *Harnessing the economic and social power of data*. Available from: https://nzdatatrust.com/

Ngāti Whātua Ōrākei Trust v. Attorney General [2022] NZHC 843.

Noble, S. (2018). *Algorithms of Oppression*. New York University Press.

Organisation for Economic Cooperation and Development (OECD). (2013). *Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data.* Available from: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

O'Neil, C. (2016). *Weapons of maths destruction: How big data increases inequality and threatens democracy*. Crown Books.

Open Data Charter. (2015). I*nternational Open Data Charter.* Available from: https://opendatacharter.net/wp-content/uploads/2015/10/opendatacharter-charter_F.pdf

Paulger, D. (2022). *New Zealand: Status of consent for processing personal data.* Asian Business Law Institute & Future of Privacy Forum. Available from: https://fpf.org/blog/new-report-on-limits-of-consent-in-new-zealands-data-protection-law

Privacy Act 2020 (NZ). Available from: https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23312.html

Privacy Commissioner. (2018). Privacy Commissioner's commentary on *R v Alsford*: Voluntary requests for personal information by law enforcement agencies. Available from: https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Guidance-resources/May-2018-Alsford-commentary-for-external-use2.pdf

Privacy Commission 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.* Available from:

https://www.privacy.org.nz/publications/commissioner-inquiries/ipcaopc-joint-inquiry-into-police-conduct-when-photographing-members-of-the-public/

Queensland Health (2022) Alcohol and Other Drug Treatment Services (AODTS) National Minimum Data Set (NMDS). Available from: https://www.data.qld.gov.au/dataset/alcohol-and-other-drug-treatment-services-aodts-national-minimum-data-set-nmds

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.

Rainie, S. C., Kukutai, T., Walter, M., Figueroa-Rodríguez, O. L., Walker, J., & Axelsson, P. (2019). Indigenous data sovereignty. In T. Davies, S. Walker, M. Rubinstein, & F. Perini (Eds.), *The state of open data: Histories and horizons* (pp. 300–319). African Minds and International Development Research Centre.

Ravindra, V. and Grama, A. (2021, June). De-anonymization attacks on neuroimaging datasets. In *Proceedings of the 2021 International Conference on Management of Data* (pp. 2394-2398). Available from: https://dl.acm.org/doi/pdf/10.1145/3448016.3457234

Research Data Alliance Indigenous Data Sovereignty Interest Group. (2019). *CARE principles for Indigenous data governance*. Global Indigenous Data Alliance. Available from: https://www.gida-global.org/care

Sandvig, C., Hamilton, K., Karahalios, K., & Langbort, C. (2016). Automation, algorithms, and politics. When the algorithm itself is a racist: Diagnosing ethical harm in the basic components of software. *International Journal of Communication*, *10*(0), 19.

Schnarch, B. (2004). Ownership, Control, Access, and Possession (OCAP) or Self-determination applied to research: A critical analysis of contemporary First Nations research and some options for First Nations communities. *International Journal of Indigenous Health*, *1*(1), 80–95.

Stats NZ (2020). *Ngā tikanga paihere: A framework guiding ethical and culturally appropriate data use*. https://data.govt.nz/toolkit/data-ethics/nga-tikanga-paihere/

Stats NZ (2021, February 12). *Mana Ōrite relationship agreement*. Available from: https://stats.govt.nz/about-us/what-we-do/mana-orite-relationship-agreement/

Solove, D. (2002). Conceptualizing Privacy. *California Law Review*, *90*(4), 1087–1156.

Solove, D., & Schwartz, P. (2011). *Information privacy law* (5th ed.). International Association of Privacy Professionals.

Sunstein, C. R. (2019). Algorithms, Correcting Biases. *Social Research: An International Quarterly*, *86*(2), 499–511. https://muse.jhu.edu/article/732187

Taylor, L. (2016). No place to hide? The ethics and analytics of tracking mobility using mobile phone data. *Environment and planning D: Society and Space*, *34*(2), 319–336. https://doi.org/10.1177/0263775815608851

Taylor, L., Floridi, L. & van der Sloot, B. (Eds.). (2017a). *Group privacy: New challenges of data technologies*. Springer International Publishing.

Taylor, L., Floridi, L., & van der Sloot, B. (2017b). Introduction: A new perspective on privacy. In L. Taylor, L. Floridi, & B. van der Sloot (Eds.), *Group privacy: New challenges of data technologies* (pp. 1–12). Springer International Publishing. Available from: https://doi.org/10.1007/978-3-319-46608-8_1

Te Arawhiti | The Office for Māori Crown Relations. (2022). *Providing for the Treaty of Waitangi in legislation and supporting policy design*. Available from: https://www.tearawhiti.govt.nz/assets/Tools-and-Resources/Providing-for-the-Treaty-of-Waitangi-in-legislation.pdf

Te Kāhui Raraunga. (2021a). *Māori data governance co-design review*. Te Kāhui Raraunga. Available from: https://www.kahuiraraunga.io/tawhitinuku

Te Kāhui Raraunga. (2021b). *Tawhiti nuku: Māori data governance co-design outcomes report.* Te Kāhui Raraunga. Available from: https://www.kahuiraraunga.io/tawhitinuku

Te Kāhui Raraunga. (2021c). *Iwi data needs*. Available from: https://www.kahuiraraunga.io/_files/ugd/b8e45c_499e6dc614cd4aa089fe9344c47701ec.pdf

Te Mana Raraunga. (2017). Te Mana Raraunga. Available from: https://www.temanararaunga.maori.nz/

Te Mana Raraunga. (2018). Principles of Māori data sovereignty. Available from: https://www.temanararaunga.maori.nz/nga-rauemi

Te Pou Matakana Limited v Attorney-General (No 1), NZHC 2942 ___ (high.court 2021). Available from: 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). Available from: https://www.courtsofnz.govt.nz/assets/cases/2021/2021-NZHC-3319.pdf

Trans-Tasman Resources Ltd v Taranaki-Whanganui Conservation Board [2021] NZSC 127. Available from: https://www.courtsofnz.govt.nz/assets/cases/2021/2021-NZSC-127.pdf

United Nations General Assembly. (1948). *Universal Declaration of Human Rights*, 10 December, 217A (III). Available from: https://daccess-ods.un.org/tmp/8527549.50523376.html

United Nations General Assembly. (1966a). *International Covenant on Civil and Political Rights*, 16 December, United Nations, Treaty Series, vol. 999. Available from: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

United Nations General Assembly. (1966b). *International Covenant on Economic, Social and Cultural Rights*, 16 December, United Nations, Treaty Series, vol. 993, p. 3.

United Nations General Assembly. (2007). *United Nations Declaration on the Rights of Indigenous Peoples: Resolution / adopted by the General Assembly* (A/RES/61/295). Available from: https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.18_declaration%20rights%20indigenous%20peoples.pdf

United Nations High Commissioner for Human Rights. (2018). *The right to privacy in the digital age* (A/HRC/39/29). Available from: https://www.ohchr.org/en/documents/reports/ahrc3929-right-privacy-digital-age-report-united-nations-high-commissioner-human

van der Sloot, B. (2017). Do groups have a right to protect their group interest in privacy and should they? Peeling the onion of rights and interests protected under article 8 of ECHR. In L. Taylor, L. Floridi, & B. van der Sloot (Eds.) *Group privacy: New challenges of data technologies* (pp. 197–224). Springer International Publishing.

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, *12*, 197–208. http://dx.doi.org/10.24908/ss.v12i2.4776

Victorian Information Commissioner. (2021). *Understanding culturally diverse privacy: Aboriginal and Torres Strait Islander peoples' perspectives* (20/11058D). Available from: https://ovic.vic.gov.au/privacy/resources-for-organisations/understanding-culturally-diverse-privacy-aboriginal-and-torres-strait-islander-peoples-perspectives/

Vis-Dunbar, M., Williams, J., & Weber Jahnke, J. (2011). *Indigenous and community-based notions of privacy: A technical report of the Informational Privacy Interdisciplinary Research Group, University of Victoria*. http://dx.doi.org/10.13140/RG.2.2.16005.14568

Waitangi Tribunal. (1999). *The radio spectrum management and development final report* (WAI 776). Available from: https://forms.justice.govt.nz/search/Documents/WT/wt_DOC_68205950/Wai776%20final.pdf

Waitangi Tribunal. (2011). *Ko Aotearoa tēnei: A report into claims concerning New Zealand law and policy affecting Māori culture and identity* (WAI 262, Vol. 1). Available from: https://forms.justice.govt.nz/search/Documents/WT/wt_DOC_68356416/KoAotearoaTeneiTT2Vol1W.pdf

Waitangi Tribunal. (2014). *He Whakaputanga me te Tiriti: The Declaration and the Treaty: The report on stage 1 of the Te Paparahi o Te Raki Inquiry* (WAI 1040). Available from: https://forms.justice.govt.nz/search/Documents/WT/wt_DOC_85648980/Te%20RakiW_1.pdf

Waitangi Tribunal. (2019). *Hauora: Report on stage one of the health services and outcomes kaupapa inquiry* (WAI 2575). Available from: https://forms.justice.govt.nz/search/Documents/WT/wt_DOC_152801817/Hauora%20W.pdf

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

Wallace, S. E., Gourna, E. G., Nikolova, V., & Sheehan, N. A. (2015). Family tree and ancestry inference: Is there a need for a 'generational' consent? *BMC Medical Ethics*, *16*(1), 87. https://doi.org/10.1186/s12910-015-0080-2

Walter, M., Kukutai, T., Carroll, S. C., & Rodriguez-Lonebear, S. (2020). *Indigenous data sovereignty and policy*. Routledge. https://doi.org/10.4324/9780429273957

Weber, M., Yurochkin, M., Botros, S., & Markov, V. (2020). *Black loans matter: Fighting bias for AI fairness in lending*. MIT-IBM Watson AI Lab.

Wicks, A. C., Budd, L. P., Moorthi, R. A., Botha, H., & Mead, J. (2021). *Automated hiring at Amazon* (SSRN Scholarly Paper ID 3780423). https://dx.doi.org/10.2139/ssrn.3780423

Williams, H., Vis-Dunbar, M. & Weber, J. (2011). First Nations privacy and modern health care delivery. *Indigenous Law Journal, 10*, 101–32. https://jps.library.utoronto.ca/index.php/ilj/article/view/27636/20367

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

Zins, C. (2007). Conceptual approaches for defining data, information, and knowledge. *Journal of the American Society for Information Science and Technology*, *58*(4), 479–493. https://doi.org/10.1002/asi.20508

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Public Affairs.

Appendix 1: Data risks

Sharing of Data

A common consideration is that an individual may share specific personal information – for example, a photo – directly with another specific person and such information will be restricted to those individuals. The assumption is that such information will be restricted and only held between these people unless the participants agree otherwise. There is an expectation that such information will not be shared outside without consent or sold to private or government actors. Any interference with such information will only be in exceptional circumstances and with a legal and ethical basis. Such assumptions no longer hold in the digital sphere, in particular, where mechanisms trawling large amounts of data including information people considered personal and only shared between specific people.

Big Data

Data risk and privacy issues arise from 'big data'. Big data can refer to almost any information-processing involving very large data sets, often involving millions or billions of people (or other entities) with thousands or millions of data points per person. Although the term emphasises data, the algorithms used to analyse the data are equally important: artificial intelligence and machine learning algorithms can be applied to allow the system to learn and adapt the algorithm based on the data. The application of big data includes technologic practices, epistemologies and ontologies. Big data creates a risk of detailed profiles about a person or a group of people, based on numerous data points across different domains. The algorithm itself may 'learn' biases inherent in the data (Kuhlman et al., 2020; Sunstein, 2019), which is particularly concerning when automated systems are used to make decisions affecting people.

Big data analytics and tools challenge the "fundamental basis of the social, legal and ethical practices and theories that have been developed and applied over decades" (Taylor et al., 2017b, p. 5). For example, they challenge the idea of what constitutes a 'valid reason' for a decision on issues such as granting parole or credit. A crucial aspect of these systems is that they work only if those administering them have access to vast quantities of data. Much of this data derives from platforms that offer services to consumers but the main value for the company/organisation comes from the harvesting of personal details and information of the consumers. Consumers click the 'accept button' knowing that they need the service despite the lack of control that they have or over where the data will go (Lee & Zong, 2019). In spite of this, technology platforms argue that consumers have made an informed choice (Lee & Zong, 2019). This introduces a tremendous asymmetry in power: those with

access to data can implement sophisticated analytics to derive valuable insights from it, which improves their position of power (Eubanks, 2018; Noble, 2018).

ANONYMISED AND AGGREGATED DATA

Another issue that arises is legal protection of anonymised and aggregated social data, and data about inanimate objects or natural phenomena. There is a growing literature that focuses on re-identification of individuals. For example, it is possible to make inference of personal attributes and predict the sexual orientation of a person through their social media usage, or even identify friendships outside of a social network platform (Garcia et al., 2018, p. 2). Protection for such data is important as there are both individual and collective privacy issues with the data. There have consequently been a series of (sometimes highly sensitive) data sets released in the belief that they were de-identified, only to have easy individual re-identification demonstrated (Culnane et al., 2017, 2019; Joly et al., 2015; Narayanan et al., 2011; Narayanan & Shmatikov, 2008, 2019; Ravindra & Grama, 2021).

There are clearly implications for open data, even if individuals cannot be identified. If, for example, the data allows identifiable groups to be distinguished, and inferences made about them in an aggregate sense – for example, that a certain group has a very high rate of a certain health condition – then this could affect the group of people even if explicit information about individuals remains hidden. This certainly affects Indigenous people, often more seriously than the rest of the population. For example, the Queensland Government publishes a detailed data set of individual records of people who sought help for alcohol and other problems (Queensland Health, 2022). Many people are easily identifiable in this data set as a result of their age range, postcode and other details. However, Indigenous people are much more likely to be identifiable, because the data set records three different types of Indigenous status (and only one large category for all non-Indigenous people), so some Indigenous people are grouped with only a very small number of others. This makes their record very easy to identify from only a small amount of other information about the person. So while re-identification is a risk for all people whose records are in the data set, the risk is much more severe for Indigenous people because they belong to small identifiable minorities.

SURVEILLANCE

Though government surveillance is not new, its capacity and intensity has increased, particularly since the 9/11 attacks. Though it is the State that has mandated such surveillance, much of this has been outsourced to the private sector (Crampton, 2015, p. 528). These companies have little transparency in how they cooperate with State surveillance, what the intended data to be collected is, and sometimes how they are funded (Crampton, 2015, p. 528). Moreover, since many of these are global companies, their capture is also international, reaching beyond the border of the State mandating such surveillance regulations. Companies such as Facebook, Google and Microsoft have users worldwide, and the USA

for example, through such companies, not only has access to the data of US citizens, but also of those using these platforms around the world. So do Chinese companies such as Huawei and TikTok.
A recent study of Twitter showed that even those who are not users of the social media platform (and who thus did not agree to its privacy policy) could still be personally identified (Garcia et al., 2018, p. 2). The mechanism is simple: people post personal information (such as photographs) of the other people they interact with, thus giving Twitter information about those who do not use it. “The implications of our results are clear: individuals do not have full control over their privacy and the decision not to share information with an online service is mediated by the decisions of other people. This means that we cannot conceive online privacy as a purely individual phenomenon that can be reduced to the decisions of a person” (Garcia et al., 2018, p. 11). Another more challenging example is the successful identification of serious criminals using the voluntarily uploaded DNA of their relatives (Garner & Kim, 2018–2019; May, 2018; Wallace et al., 2015).