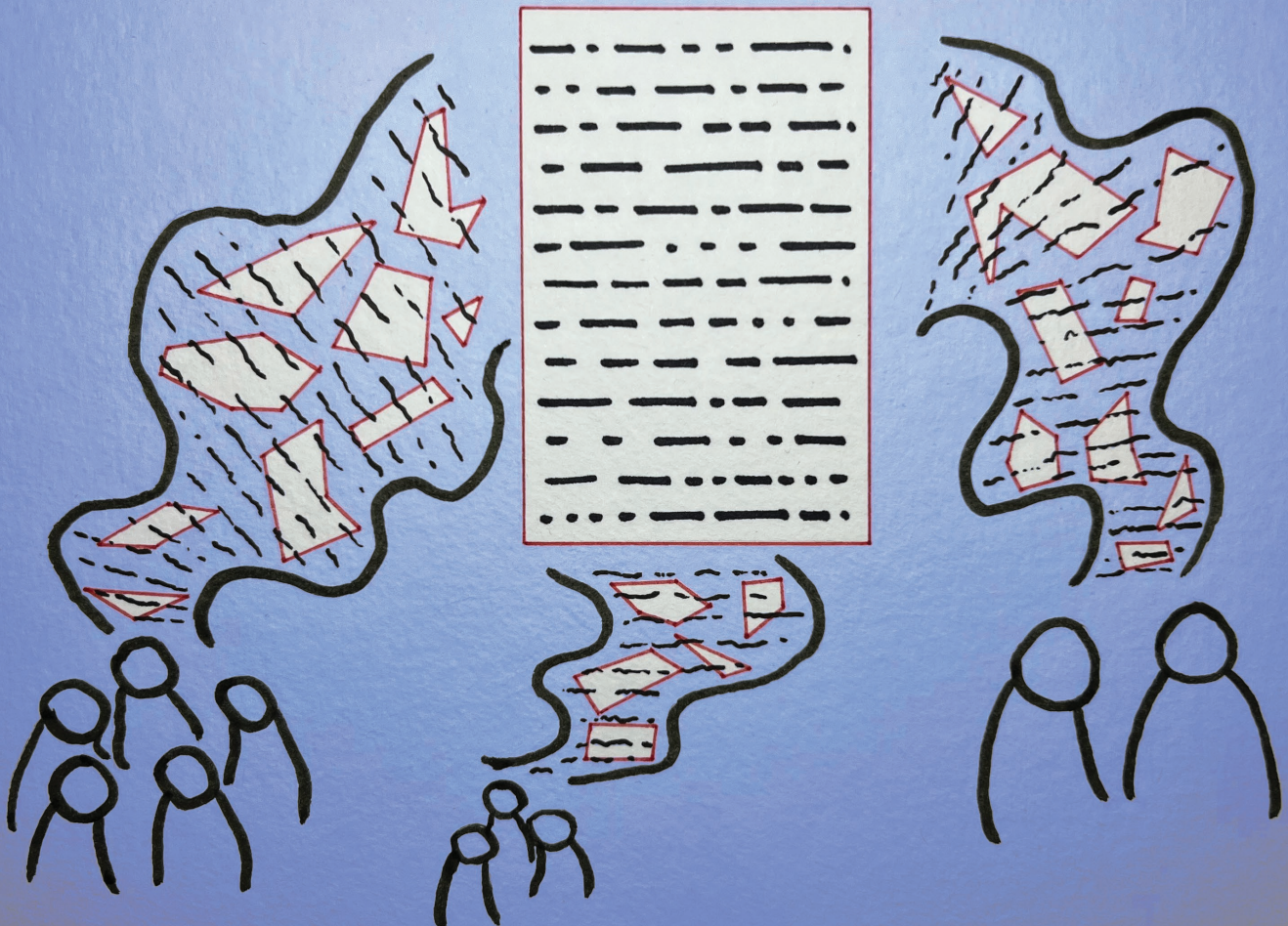




Te Kāhui Tika Tangata
Human Rights Commission



AI and Digital Technologies:

A Human Rights and
Te Tiriti o Waitangi Approach

About Te Kāhui Tika Tangata Human Rights Commission

Te Kāhui Tika Tangata Human Rights Commission is Aotearoa New Zealand's national human rights institution (NHRI), operating under the UN Paris Principles.

The Human Rights Commission was formed in 1977 to provide better implementation and protection of human rights in Aotearoa New Zealand. The Commission works under the Human Rights Act 1993.

The Commission is funded through the Ministry of Justice but operates independently of the New Zealand Government as an independent Crown entity.

We are the voice for human rights in Aotearoa New Zealand. Our vision is to be a credible, effective, connected and highly valued organisation that makes human rights and the human rights dimensions of Te Tiriti real and relevant. We are confident in our Tiriti-based aspiration and are working to make a positive impact for all communities, individuals, whānau, hapū, and iwi in Aotearoa New Zealand.

Citation

Te Kāhui Tika Tangata New Zealand Human Rights Commission. (2026) AI and Digital Technologies: A Human Rights and Te Tiriti o Waitangi Approach. Wellington, Human Rights Commission.

ISBN: 978-0-473-79816-1 (print)

ISBN: 978-0-473-79815-4 (online)

Te Kāhui Tika Tangata Human Rights Commission

Creative Commons License: Attribution — Non-Commercial — Share-Alike 4.0 International

Published August 2026

Acknowledgements

The Commission is grateful to the members of the expert advisory group for the time, expertise, and thoughtful feedback they provided on earlier drafts of this report. We are also grateful to the three independent reviewers whose constructive feedback strengthened the final report. This work has also been informed by engagement with a wider group of local and international experts, whom we would like to thank for their contributions.

We would also like to acknowledge the research undertaken by Tom Barraclough of Brainbox, and the additional writing and editing support provided by Anna and Kelly Pendergrast of Antistatic.

Finally, the Commission would like to thank the members of its internal team involved in writing this report: Sophie Bradwell-Pollak, Julie Corker, Eleanor Vermunt and Esther Rootham. Their expertise, commitment, and support were fundamental to the development of this report.

Executive summary

Aotearoa New Zealand can be a society in which our governance of, access to, and use of digital technologies supports dignity, equality, and participation for all. Digital technologies, particularly artificial intelligence (AI), are rapidly reshaping how people live, work, and participate in society. These technologies are becoming increasingly embedded in everyday life — from public services and workplaces to education, health, and communication.

AI and digital technologies are often approached as discrete tools or market products. This report finds that AI and digital technology systems are better understood as infrastructure. Recognising AI and digital technologies as infrastructure has important implications. Infrastructure requires deliberate design, long-term planning, and public accountability. It should be governed in ways that are transparent, equitable, trusted and designed to enhance the public good.

Te Kāhui Tika Tangata Human Rights Commission (the commission) emphasises that realising this vision of society where technology enhances wellbeing requires governance that is firmly grounded in human rights and Te Tiriti o Waitangi. Our encounters with AI and digital technologies engage a wide range of human rights, including rights related to privacy, non-discrimination, access to information, work, health, and culture. The report recognises that human rights are both individual and collective. People's interactions with AI and digital technologies engage these rights at multiple levels, affecting individuals directly while also creating impacts for communities and groups, particularly in relation to data, culture, and decision-making. Whenever human rights are impacted, a methodology for understanding and managing that impact is required.

A human rights and Te Tiriti-based approach provides a framework to guide how these technologies are designed, deployed, and governed, so that their benefits are realised and their risks are addressed.

While the analysis in this report extends to all digital technology systems it has a specific focus on AI, reflecting that these tools are increasingly embedded in our daily lives and are current topics of public discussion and concern. This report adopts the OECD definition of AI:

An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.¹

A human rights and Te Tiriti-based approach

Aotearoa New Zealand does not need to develop an entirely new framework for governing AI and other digital technologies. A comprehensive foundation already exists in international human rights law, domestic legislation and Te Tiriti o Waitangi, which together form a human rights framework for Aotearoa New Zealand.

Te Tiriti o Waitangi is central to the governance of AI and digital technologies as infrastructure in Aotearoa New Zealand as it affirms the partnership between Māori and the Crown, and requires the active protection of Māori rights and interests. This means, at a minimum, that Māori must have meaningful influence over how systems are governed and used, and Māori data sovereignty must be recognised as foundational to any national approach.

A human rights-based approach (HRBA) provides a practical, internationally-recognised method for applying this framework. It involves identifying the rights at stake, assessing impacts, and ensuring that decisions are lawful, proportionate, and accountable. It is operationalised through the following principles, which form the acronym:

- Participation
- Accountability and transparency
- Non-discrimination and equality
- Empowerment
- Legality.

In the context of digital infrastructure, taking a HRBA means embedding the principles into the design, development, deployment, and governance of systems, rather than applying them retrospectively.

Human rights risks and opportunities

AI and other digital technologies impose real risks on rights, including risks at scale. They also create real opportunities to advance human rights, including for people whose rights have historically been undermined. This report addresses both the risks and the opportunities — identifying what must be protected, what should be promoted, and what structural changes are needed to make both possible.

Key human rights risks include:

- privacy breaches, intrusive data collection, misuse, misappropriation and unconsented use of personal data,
- discrimination and bias in automated decision-making,
- digital exclusion limiting access to services and participation,
- lack of transparency, accountability, and access to remedy,
- job displacement and impacts on work,
- misuse of Māori data and risks to Māori rights and interests, and
- environmental impacts of digital infrastructure.

At the same time, the opportunities are significant. AI and digital technologies can potentially:

- improve access to healthcare, education, and public services,
- enhance accessibility for disabled people,
- strengthen transparency and access to information,
- enable community empowerment and participation,
- support the revitalisation of te reo Māori and indigenous knowledge, and
- expand access to the benefits of scientific and technological progress.

This report finds that these outcomes are not guaranteed, and highlights the importance of having governance approaches that reflect human rights and Te Tiriti o Waitangi.

Shared responsibility

The governance of digital infrastructure is a shared responsibility, reflecting both its system-wide impacts and its development across public and private domains.

- The **government** has primary responsibility to respect, protect, and fulfil human rights, and to give effect to Te Tiriti o Waitangi through law, policy, investment, and public service delivery.
- **Māori**, as Tiriti partners, in exercising their right to self-determination, must have meaningful and ongoing roles in shaping how digital infrastructure is designed, governed, and used, including in relation to data and decision-making systems.
- The **private sector** must undertake human rights due diligence and risk mitigation to ensure that the technologies it develops and deploys do not cause potential or actual human rights harms.
- **Communities and civil society** play a critical role in identifying impacts, informing design, and holding institutions to account.

This system-wide approach reflects that digital infrastructure is shaped by choices in its design and governance. Supporting inclusive, accountable, and Tiriti-consistent outcomes involves participation and leadership across government, Māori, the private sector, and communities.

Recommendations

To develop a more coordinated approach and place human rights and Te Tiriti o Waitangi at the centre of digital infrastructure, the commission makes two central recommendations to the Government:

Recommendation One: Develop a national digital infrastructure strategy anchored in human rights and Te Tiriti o Waitangi

The commission suggests the following key actions:

- Develop a whole-of-society national digital infrastructure strategy with explicit human rights and Te Tiriti foundations and that upholds Māori data sovereignty, on a long-term planning horizon that matches the country's other infrastructure planning, and enables our digital sovereignty.
- Establish one point of accountability to advance and coordinate the development of the strategy.

Recommendation Two: Develop a national approach to risk assessment and mitigation for AI and digital technologies, anchored in human rights and Te Tiriti o Waitangi

The commission suggests the following key actions:

- Adapt existing Aotearoa New Zealand frameworks and draw on international best practice in developing the national approach to human rights and Te Tiriti risk assessment and mitigation.
- Include both public and private sector entities in its scope.
- Adequately resource the commission, as Aotearoa New Zealand's independent national human rights institution, to play a leadership role in the development of a national human rights and Te Tiriti-based risk assessment for AI and digital technologies.
- Ensure this work is done in partnership with Māori and their representative organisations as Te Tiriti-rights holders, and with other relevant independent crown agencies.

System Enablers

In addition to the recommendations, the report identifies three system enablers to support the consistent application of a human rights and Te Tiriti-based approach to AI and digital technologies.

System Enabler One: Empower people and communities to shape how AI affects their lives

The report emphasises that a rights-based approach depends on people and communities being able to understand, engage with, and influence how AI and digital technologies affect their lives. Practical steps include:

- supporting iwi and hapū to exercise their self-determination, particularly in relation to **Māori data sovereignty**,

- advancing **digital inclusion**, including access, affordability, capability, and targeted support for underserved communities,
- ensuring **AI, and human rights and Te Tiriti o Waitangi literacy**, so people understand how systems affect them and what rights and choices they have,
- encouraging publication in **machine-readable formats** to support the use of digital systems, and to enhance accessibility for disabled people,
- supporting **equitable workforce transitions** including through research and by identifying impacts on workers and responding where appropriate,
- supporting a **rights-respecting technology sector**, including by incentivising AI development that benefits society,
- evaluating the role of Aotearoa New Zealand in promoting **Pacific data sovereignty**.

The report also highlights that meaningful engagement requires accessible information, real influence over decisions, and the capability to participate effectively, rather than consultation alone.

System Enabler Two: Government leadership and accountability

The public sector plays a critical role in shaping digital infrastructure through policy, regulation, procurement, and service delivery. Key areas for impact include embedding human rights and Te Tiriti o Waitangi in decision-making processes by:

- upholding **Māori data sovereignty**, including Māori involvement in governance and oversight,
- ensuring **non-digital channels for essential public services** to the extent possible,
- requiring **participatory engagement** in design, deployment and evaluation of digital systems,
- embedding **rights-based public procurement** of AI and digital technologies and using **procurement and investment as levers**, including requiring rights and Tiriti-based impact assessment for digital systems,
- ensuring accessible **individual and collective complaints and accountability mechanisms**,
- implementing a **national register of algorithms used in the public sector**,
- establishing an **AI harm reporting and monitoring system**, and
- establishing an **AI Safety Institute**, responsible for providing technical evaluation and oversight of AI systems, and connecting with the international network of safety institutes.

Strengthened leadership will help ensure that digital infrastructure reflects shared public values and supports equitable outcomes.

System Enabler Three: Addressing legislative and regulatory gaps

Existing legal and regulatory frameworks do not yet fully address the risks associated with AI and digital technologies. The report identifies the need for action by:

- enforcing **rights to accessibility of digital systems** to ensure AI and digital systems in the public service do not exclude disabled people,
- addressing **non-consensual sexual deepfakes** through urgent legislative action,
- strengthening **transparency and accountability in public service** including by clarifying how legal obligations apply to automated systems,
- addressing risks associated with digital technologies, including risks posed to critical **cyber infrastructure**, and those posed by **ambient surveillance devices** such as smart glasses,
- advancing a **graduated approach to regulating social media platforms**, grounded in human rights,
- considering the responsibilities and **liability of transnational technology providers**.

An invitation to shape the future

Digital infrastructure will play an increasingly significant role in shaping how people in Aotearoa New Zealand live, work, and participate in society. The values embedded in these systems will influence how opportunities, risks, and responsibilities are distributed.

This report highlights the importance of deliberate and coordinated action: to recognise AI and digital technologies as infrastructure, to ground their governance in human rights and Te Tiriti o Waitangi, and help ensure that technological change supports dignity, equity, and wellbeing for all.

Foreword: Dr Stephen Rainbow

Chief Human Rights Commissioner

This report presents a vision of a future where artificial intelligence (AI) helps Aotearoa New Zealand thrive, shaped by our shared values, grounded in human rights and Te Tiriti o Waitangi, and creating opportunities for all.

Every day brings a new claim about AI. Governments point to its economic promise. Others warn of serious risks: inequality, job displacement, and decisions moving beyond meaningful human control. AI may help detect breast cancer; it may also deepen existing discrimination in access to services for specific groups. So, what are we to believe?

A rights-based approach requires us to hold both truths together. Human rights are not a brake on innovation, but guardrails to help innovation serve people, build public trust to ensure the public know risks are being managed, and prevent harm.

At a time when the international system faces significant uncertainty and financial strain, the international human rights framework remains the vital source of guidance, providing a clear set of principles that offer both direction and certainty for governments, businesses, and communities navigating the opportunities and risks of AI and other digital technologies.

The technology, business models, and rules around AI are changing quickly. That pace can make the future feel inevitable. It is not. The choice is whether Aotearoa New Zealand shapes AI deliberately and democratically, or drifts into decisions driven by procurement, market pressure, and poorly understood systems. This report argues for conscious choice grounded in human rights. Human rights give us a baseline when technology feels new, complex, or contested. They require us to ask: Who has access to the benefits of AI and digital technologies? Who is harmed? Who has a say? Who is accountable?

Australia's emerging approach to AI governance, including the establishment of an Office of AI, the development of a National AI Plan, and moves toward legislated AI standards, marks an important development in our region, and we look forward to seeing how its implementation unfolds in practice and what lessons may be drawn for the protection and promotion of human rights.

Our report makes two central recommendations: a national digital infrastructure strategy, and a national approach to risk assessment and mitigation, both anchored in human rights and Te Tiriti. Te Tiriti o Waitangi is part of our domestic human rights framework and it is important that all of us, not just Māori, ensure that it is upheld in relation to the way we govern these rapidly evolving digital technologies.

This work cannot be carried by the government alone. Iwi and hapū, communities, disabled people, children and young people, workers, businesses, researchers, regulators, civil society, and those most affected by digital systems all have a role. Participation is part of making technology trusted and trustworthy.

To research and draft this report, Te Kāhui Tika Tangata Human Rights Commission has benefited from the insight and generosity of many people across Aotearoa New Zealand and internationally, and our remarkable External Advisory Group. On behalf of the Board, I thank everyone who shared their expertise, hopes, and concerns. The report remains the commission's responsibility but is stronger because of those contributions.

This paper is an invitation to put rights at the centre of AI and digital infrastructure, and to ensure technological change contributes to he whakamana tangata, a life of dignity for all.

Foreword: Dayle Takitimu

Rongomau Taketake Indigenous Rights

Governance Partner

Ko te Tiriti o Waitangi te tūāpapa o te kāwanatanga i Aotearoa, ā, e mau tonu ana ngā kawenga katoa i raro i tā tātou kawenata tapu. Ko te tino rangatiratanga o ngā iwi me ngā hapū e kore e memeha, ahakoa te aha. Ko te wero i mua i a tātou; ko te whakatinanatanga o ēra kupu nui, i ngā wā katoa, i ngā wāhi katoa, i ngā kaupapa katoa, mō te ora pai o te katoa.

At a time when AI and other emerging digital technologies are increasingly shaping the systems we rely on every day, this report makes a compelling case for understanding them as a form of public infrastructure with constitutional and human rights significance. It sets out how Aotearoa New Zealand can take a thoughtful and principled approach to governing this infrastructure in ways that uphold human rights, honour Te Tiriti o Waitangi, and support the dignity and wellbeing of all. In doing so, it highlights both the significant opportunities these technologies offer and the importance of shaping their development in ways that manage risks early and well.

This approach is closely connected to Aotearoa New Zealand's wider constitutional conversation about how authority is shared and exercised. The Waitangi Tribunal in *He Whakaputanga me te Tiriti* (Wai 1040, 2014) affirmed that the rangatira who signed in 1840 did not cede their sovereignty. The High Court in *Te Pou Matakana Limited v Attorney-General* confirmed the practical consequence: a statutory power that engages Māori interests must be exercised in accordance with Te Tiriti, even where the governing statute carries no express Tiriti clause. This recognises the enduring nature of Tiriti obligations — they are neither optional nor able to be cherry picked. In practice, in the AI and digital technology space, this means the Crown is legally obliged to engage with Māori as tangata whenua and Tiriti partners in decisions about the development and governance of digital technologies such as AI.

In this context, Te Tiriti o Waitangi and human rights — particularly the right of Indigenous peoples to self-determination — must be understood as foundational to the governance of AI and related technologies. These are not peripheral considerations. They are necessary preconditions for lawful, legitimate, and effective regulatory frameworks. The right to free, prior and informed consent, as reflected in international human rights standards, is directly engaged where AI systems, data practices, and digital infrastructure affect Māori rights and interests. Its practical implementation will be critical to ensuring that these technologies are developed and deployed in ways that are consistent with both Te Tiriti and Aotearoa New Zealand's international commitments.

Recognising AI as infrastructure also presents an opportunity to do things differently. Public infrastructure has too often been developed in ways that contributed to the alienation of Māori land and resources. A Tiriti-consistent approach reaffirms the pre-conditions for new technological systems to support tino rangatiratanga, equitable outcomes, and shared benefit. This will necessarily include careful consideration of the environmental demands associated with new and emerging digital technologies, which will undoubtedly have direct implications for Māori rights and interests, including in relation to whenua, wai, and other taonga.

Ensuring meaningful Māori engagement is therefore both a legal obligation and a pathway to better outcomes. Māori expertise, values, and governance approaches are already shaping leading practice in this area. Initiatives such as Te Pā Tūwatawata, led by the Data Iwi Leaders Group, and Te Kāhui Raraunga's Māori AI Governance Framework demonstrate how data sovereignty, accountability, and collective benefit can be embedded in the design and oversight of technological systems. While grounded in Māori rights and aspirations, these approaches have broader relevance for strengthening governance across the sector and are widely held in high regard for that very reason.

I acknowledge with appreciation the members of the Expert Advisory Group, and the wider community of contributors, whose insight and experience have informed this report. The generosity of those working in industry, in academia, with vulnerable populations, and at the intersection of Te Tiriti, Indigenous rights, and data sovereignty have materially strengthened both the depth and integrity of this work.

We trust this report makes an important and timely contribution to a critical area of public policy. Its central message is clear: the long-term success, legitimacy, and social licence of artificial intelligence in Aotearoa New Zealand will depend on our willingness to give robust and practical effect to Te Tiriti o Waitangi and to the human rights standards we have already committed to uphold.

It has been a privilege to contribute to this work, and I commend the report to those responsible for shaping the future of AI governance in Aotearoa New Zealand.

Contents

Executive summary	1
Foreword: Dr Stephen Rainbow	7
Foreword: Dayle Takitimu	8
About this report and its authors	12
Introduction: Artificial intelligence, digital technologies, human rights, and Te Tiriti o Waitangi	13
Digital technology as infrastructure for the public good	14
A human rights and Te Tiriti-based approach to AI and digital technologies	15
Why now?	16
An invitation to action	17
Introduction to AI and digital technologies.....	18
Scope of technologies covered by the report	18
AI and other digital technologies are part of a wider system	20
Introduction to New Zealand's human rights framework	21
Aotearoa New Zealand already has a human rights framework	21
Implementing a human rights-based approach	23
The human rights risks and opportunities of AI and digital technologies	32
Key human rights engaged and the attendant risks	32
The opportunities: how AI and digital technologies can promote and protect rights..	43
The rights foundation for promoting AI and other digital technologies.....	48
Who is responsible for realising human rights in relation to AI and digital technology?	49
States' core human rights obligations	49
The private sector's human rights responsibilities	51
Collective and individual rights holders	52
Whole-of-society action to balance the opportunities and risks	53
How this approach informs our recommendations	55
Actions to bring effect to a rights-based approach to AI and digital technologies	56
Overview of recommendations and priority areas for action	56

Recommendations.....	58
Recommendation One: Develop a national digital infrastructure strategy anchored in human rights and Te Tiriti o Waitangi	58
Recommendation Two: Develop a national approach to risk assessment and mitigation for AI and digital technologies, anchored in human rights and Te Tiriti o Waitangi	63
System enablers to support a rights-based approach to AI and digital technology	67
System Enabler One: Empower people and communities to shape how AI affects their lives	67
System Enabler Two: Government leadership and accountability	70
System Enabler Three: Addressing legislative and regulatory gaps.....	72
Appendix One: Engagement to support the development of this report	77
Appendix Two: AI methodology	79
End Notes	80

About this report and its authors

This report provides the reasoning and evidence base to support a responsible, fair and rights-respecting pathway for designing, building, and deploying digital technology, with a specific focus on AI and other emerging digital technologies. We intend that this report will inform a national discussion by synthesising evidence and international practice, identifying key questions, risks, and opportunities, and providing accessible guidance for diverse communities and decision-makers. While Te Kāhui Tika Tangata Human Rights Commission (the commission) does not have the mandate to make binding recommendations, the human rights principles and standards and Te Tiriti obligations that we discuss and draw on do come with binding obligations in both law and practice.

The recommendations and advice offered were developed with the support of an Expert Advisory Group (EAG) of members with expertise spanning AI and human rights, Te Tiriti o Waitangi, Indigenous rights, digital rights, ethical AI, machine learning, and the lived experience of communities adversely impacted by AI systems. The EAG met between March and May 2026 and operated under a co-chair model led by the Chief Commissioner and the commission's Rongomau Taketake Indigenous Rights Governance Partner. Engagement with a wider range of experts domestically and internationally also informed this report. A list of those we engaged is available as an **Appendix One**.

Some of the underlying research was conducted by Tom Barraclough and the Brainbox team using an AI-assisted methodology and supported by the commission's legal analysis of Te Tiriti o Waitangi and human rights law and practice. Additional writing and editing work was done by Anna and Kelly Pendergrast at Antistatic. A full methods and transparency statement is attached as **Appendix Two**.

This report is a snapshot in time. The technology will move, the deployments will move, and the governance response will move with them — but the human rights and Te Tiriti o Waitangi-based framework will not. Human rights frameworks are technology agnostic, and can be applied no matter the tool or technology in question. The framework's foundations are fixed, and its application will continue to develop in the way the common law, tikanga, and the international human rights framework have always developed. The next version of this conversation will build on this one.

Introduction: Artificial intelligence, digital technologies, human rights, and Te Tiriti o Waitangi

At Te Kāhui Tika Tangata Human Rights Commission (the commission), we recognise that everyone has the right to dignity, equality, and respect. Our role under the Human Rights Act 1993 is to advocate and promote respect for human rights in Aotearoa New Zealand as reflected in Te Tiriti o Waitangi and New Zealand's domestic and international obligations. These include civil, political, economic, cultural and social rights.

Human rights provide an internationally recognised framework for navigating periods of technological and social transformation, grounded in enduring principles that are technology-neutral and capable of responding to new and emerging challenges.

A key part of our role is providing advocacy, advice, education, and guidance on issues that affect people's everyday lives. As AI and other digital technologies increasingly shape how people work, access services, participate in society, and exercise their rights, understanding their human rights and Te Tiriti implications is an important part of that work.

This report sets the agenda for informed, collective progress towards the use of human rights-respecting, Tiriti-consistent approaches to AI and digital technologies in Aotearoa New Zealand. It contains recommendations focused on ensuring the best possible outcomes for our communities as we engage with substantial technological and social change.

We are living in a time of fast-moving technological change. In the past decade, the group of technologies known as 'AI' have become more embedded in our daily lives, and are increasingly topics of public discussion and concern. The term AI covers a broad range of techniques, including machine learning and knowledge-based approaches, and a range of application areas such as computer vision, natural language processing, speech recognition, intelligent decision support systems, and intelligent robotic systems.²

The development and use of AI tools and other digital technologies offer significant opportunities to protect and promote human rights, and in some cases to potentially increase the productivity, creativity, and wellbeing of people and communities in Aotearoa New Zealand. However, there are also risks alongside each opportunity, and these must be considered in tandem when making decisions about how AI and emerging digital technology should be regulated, funded, and deployed.

The opportunities and risks are not hypothetical — AI and emerging digital technologies are already part of everyday life in Aotearoa New Zealand. For most of us, even a simple act like taking a photo on our phone camera engages AI-driven post-processing to enhance the images. Spreadsheets, email clients, search engines, navigation apps, customer-service chatbots, and recommendation systems all use AI, and the public and private sectors alike are increasingly using AI tools to increase efficiency and improve productivity. The change is already here. Governance frameworks must be designed for the world as it is, not for a world in which AI can simply be turned off.

To realise the benefits on behalf of all people, it is essential that AI and digital technology are trusted and trustworthy.³ A 2025 University of Melbourne study⁴ found that people are more willing to use and trust AI when its governance mechanisms are considered trustworthy. Other factors that were found to impact use include the extent to which people feel they understand AI and expect benefits to arise from its use. Without responsibility and accountability, and where confidence in oversight is weak, trust and willingness to engage are lower. For those advocating the adoption of AI as a means to grow economic opportunities, this lack of trust is a significant impediment to the uptake of AI.⁵

To ensure that AI and other digital technologies are developed and deployed in ways that benefit all communities, it is crucial to address meaningful digital access more generally. The Digital Equity Coalition Aotearoa New Zealand (DECA) records that at least one in ten people in Aotearoa New Zealand are digitally excluded⁶ and over one in five struggle to access necessary services to get on with life, with the harm concentrated on families on low incomes, seniors, Māori, Pacific peoples, disabled people, those new to Aotearoa New Zealand, and remote communities.⁷ Also contributing to disparities in access to benefits of digital technologies are the uneven access to safe online environments which can limit people's ability to participate fully in an increasingly digital society. Online harms are not distributed evenly, with a recent New Zealand study finding that disabled people, followed by Māori, are most likely to have experienced online harm or harassment.⁸ Women, people over 70, and Pacific peoples have higher concerns about the security of their data.⁹

Good outcomes will not happen by chance. They result from deliberate action to empower people and communities with genuine choices and fair and just ways to participate. They demand reliable, consistent, transparent standards for the use and governance of AI and digital technology. And they rely on practical infrastructure to support the consistent application of a human rights and Te Tiriti lens to processes and decisions involving AI and digital technology. If enacted, the recommendations in this report will help to create the conditions under which people and communities can benefit from these technologies on their own terms.

Digital technology as infrastructure for the public good

A national approach to AI and digital technologies should treat these systems as public infrastructure with the purpose of serving the public good. Like roads, water systems, schools, and courts, digital technologies shape the choices people have, what people can do, who they can reach, what they can know, how power is exercised, and by whom. Infrastructure embeds the values of the people who design and govern it into everyday life — deliberately or by default. In the case of AI and digital technology, 'infrastructure' encompasses both physical structures, such as

telecommunications networks, as well as broader social and technical structures within which it operates. A public good approach to AI and emerging digital technologies takes an active, attentive approach to the human dimensions and experience of technological change.

This approach means recognising:

- the right we all enjoy, no matter who we are, to participate in our communities and make decisions in ways that are accessible and affordable,
- the responsibility of our elected and appointed officials and institutions to be accountable to the public they serve, and protect against harms by private entities such as technology companies, and to hold individuals and entities to account for human rights harms,¹⁰
- the importance of equitable access to AI and new technologies, and the ongoing work required to create a fair and just system that enables each and every one of us to benefit from technology, free from discrimination,
- the constitutional significance of Te Tiriti o Waitangi as our founding document, with equal application to digital as to tangible experiences, and
- the importance of balancing rights fairly, and ensuring that any limitations on rights are lawful, necessary and proportionate, and able to be challenged through independent processes.

Human rights standards and obligations and Te Tiriti o Waitangi together provide a robust, consistent framework for this work. They offer an approach to engaging with social and technological change that reflects a proud tradition of acting for our common good, focuses our attention on the choices we make as a community, and allows us to move forward while protecting and respecting the unique needs of Tangata Whenua and all those who arrived later. Human rights provide the principled basis for deciding what values must be embedded in our public infrastructure, and Te Tiriti provides the constitutional basis for ensuring those decisions are made in genuine partnership with Tangata Whenua. Together, they offer a durable, enforceable foundation for choices that will have impacts on our communities for generations to come.

A human rights and Te Tiriti-based approach to AI and digital technologies

While this report deals with an experience of ‘new’ technology which is marked by rapid change, a human rights lens provides us with stability, clarity, and consistency. Human rights are non-partisan, universal, normative and legal standards: the rights they safeguard apply to everyone. Human rights law provides a comprehensive, globally accepted reference point for identifying how AI and digital technologies affect people and communities. Aotearoa New Zealand has always prided itself on playing a constructive and progressive role in shaping the international rules-based order. The international position on human rights and digital technologies is clear: the OHCHR mapping report *Mapping report: human rights and new and emerging digital technologies*¹¹ records that “any protection gaps result from gaps in implementation rather than a lack of established obligations”. Ultimately, human rights provide us with the means to advocate for an approach to digital technologies that centres people’s rights to live with dignity.

Human rights law is not limited to the specific human rights protections in New Zealand law — it encompasses the full breadth of civil, political, economic, social, cultural, collective, and Indigenous rights. Human rights standards also come with duties or obligations for different actors (known as ‘duty bearers’) to respect, promote, and realise human rights. These duties fall principally on the State but also on private actors, including businesses.

Likewise, Te Tiriti — Aotearoa New Zealand’s founding constitutional document and unique statement of human rights — provides a consistent, grounded framework for making sense of AI and digital technology in our own social and cultural context. Te Tiriti affirms the partnership between iwi and hapū and the Crown, and the Crown’s kawanatanga authority to govern its own people while guaranteeing the pre-existing tino rangatiratanga or absolute authority of hapū, without discrimination. It demands active protection of those recognised and guaranteed rights. It was a forward-looking document, and as such, it provides a framework purpose-built to provide clarity on issues of substance in times of rapid change. Meaningful engagement under Te Tiriti is the mechanism through which decisions about technology gain and maintain legitimacy, and through which the values embedded in that technology can truly reflect the people it affects.

The supportive and mutually reinforcing frameworks provided by human rights and Te Tiriti offer us the opportunity to advance how we think about AI and digital technology policy in Aotearoa New Zealand, in ways that are focused on the people and communities already affected by that technology day-to-day, and who will be most affected by digital technologies in the future. They provide space for conversation that is grounded in human diversity and reflects enduring values. By understanding AI and other digital technology as infrastructure that has the ability to work for the public good, we allow ourselves to prioritise our right as individuals and communities to make substantial and informed decisions about our current and future lives.

Why now?

The guidance in this report is timely. Generative AI, automated decision-making systems, biometric technologies and network-connected devices are being deployed across health, education, justice, welfare, immigration, and everyday commercial life, both here at home and abroad. The pace of deployment often outstrips the pace of governance. The commission’s view is that action is needed now to ensure that people’s rights are respected, protected, and fulfilled as these systems are designed, deployed, and governed. Protecting people’s human rights — to choose, to take part in public affairs, to seek and receive information, to benefit from scientific progress — demands that we act. Acting now increases our opportunities to create a firm foundation for locally appropriate, human rights and Tiriti-informed use of these technologies in multiple spheres of social and cultural life including health, education, the workplace, justice, and culture.

Finally, the domestic institutional moment is open. Both major parties have committed to action on online harms, and the report of a recent Select Committee inquiry¹² touched on a range of digital technologies beyond social media, including AI and virtual private networks. Cabinet's decision to establish a Government Digital Delivery Agency (GDDA) inside the Public Service Commission¹³ is the most significant reorganisation of New Zealand's digital institutions in twenty years. On 19 May 2026, the Ministers for Finance and the Public Service both announced an intention to restructure the public service with a baseline expectation for accelerated adoption of artificial intelligence.¹⁴ These restructuring processes provide an opportunity to set up governance mechanisms that uphold human rights and Te Tiriti.

An invitation to action

This report is the commission's contribution to a national conversation that involves everyone.¹⁵ A human rights framework, drawn from Te Tiriti o Waitangi and international and domestic human rights instruments, provides a strong foundation for action on AI and digital technologies. It is also dynamic in the way it is applied as those technologies and their uses evolve. The recommendations and system enablers described in the report outline a set of actions that will enable the human rights framework to be applied and realised in Aotearoa New Zealand — from enabling the empowerment of individuals, to the negotiation of international positions.

While the recommendations in this report are aimed at the Government to action, the work the report identifies in implementing a HRBA to AI and other digital technologies is shared work. The commission's role is to advocate for and promote respect for, understanding of, and appreciation of human rights in New Zealand society. The Government, the private sector, the public service, iwi and hapū, civil society, advocates, communities of people whose lives these technologies most directly engage, and the public all have a part to play.

Introduction to AI and digital technologies

In this section, we briefly introduce some of the key technologies covered in this document in order to build understanding and provide a conceptual grounding for the remainder of the report.

Scope of technologies covered by the report

Much of this report focuses on AI and the social and technical systems that support it. AI is one of the most transformational digital technologies of recent decades, with attendant human rights risks and potential benefits. However, AI does not function in isolation, and it is not the only digital technology with significant human rights impacts.

The commission's aim is to ensure that this report and its recommendations can be applied to other relevant technologies and be relevant in a fast-moving technological context, and as such the scope of this report reaches beyond AI to include other digital technologies. This is a broad category that includes automated decision-making systems that employ rules-based algorithms, biometric technologies, social media, and network-connected devices. This widened scope also reflects the real world harms already taking place as a result of non-AI digital technologies. Two prominent scandals of the past decade related to devastating human rights impacts on vulnerable people were the result of non-AI rule-based systems closer to traditional computer programmes.¹⁶

Artificial intelligence (AI)

While there is no single agreed definition of AI, the commission adopts the OECD definition:¹⁷

“An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.” — OECD¹⁸

Elsewhere, the OECD notes that topics typically covered by the definition above and the term ‘AI’ more generally include “categories of techniques such as machine learning and knowledge-based approaches; application areas such as computer vision, natural language processing, speech recognition, intelligent decision support systems, and intelligent robotic systems; and specific applications of these tools in different domains”.¹⁹

Ordinary software is like a set of steps that a computer follows strictly based on what a human developer has told it to do. If you read the code, you can know what the system will do. A rule-based decision system works the same way. The system is ‘deterministic’ in the sense that you can know, for any given input, what the output will be. This is in contrast to how AI systems work.

Two types of AI systems that are useful to understand in the current context are Generative AI and Agentic AI. A short overview of each is provided below.

Generative AI

Generative AI is “a type of AI system that can create or generate new content such as text, images, video and music based on models and patterns detected in existing datasets”.²⁰

Generative AI tools used to generate text and code, like ChatGPT or CoPilot, are underpinned by large language models. These are neural networks designed to predict the next word in a sequence across an enormous body of data, and trained to improve those predictions based on human feedback. What it stores is not the training data itself, but a statistical map of patterns distributed across billions of data points or parameters. A generative AI system produces outputs by sampling from that map in response to a prompt. Unlike ordinary software, generative AI systems are ‘non-deterministic’. The model may produce different outputs every time, even in response to the same prompt. There is also no rule the developer can point to, and no reliable way to predict what the model will produce on inputs it has not seen.

Large language models are produced through a multi-stage pipeline:

- **Pre-training**, which takes an enormous corpus of text — most of the public web that can be scraped, plus selected books, code, and reference material — and trains a neural network to predict missing or next words, repeated trillions of times. The collected materials over-represent English, the views of online-active populations, and well-resourced institutions. Once a model is trained, individual training items cannot meaningfully be removed.
- **Post-training**, which shapes the pre-trained model using a smaller and more carefully curated dataset. It involves ‘fine-tuning’ the model’s weights to target a particular domain or task, or to ‘align’ the model’s outputs with those the developer wants to adhere to. Techniques such as reinforcement learning from human feedback determine what a model may refuse to do, the tone of its outputs, and the positions it takes on particular issues, and new techniques and practices are evolving all the time. The training process can sometimes be performed by a global workforce of annotators concentrated in the global South, whose rights may be infringed in the course of their work, without adequate redress.²¹
- **Deployment**, which is where most current governance levers sit: safety evaluation, systems that identify harmful outputs and impose guardrails, the application that wraps the model in a user interface, and the institutional decisions about where and how the model is used.

Agentic AI

Agentic AI describes an arrangement in which a large language model is given access to tools and methods that let it take actions on a user's behalf: browse the web, read and write files, run code, send messages, and interact with other software systems. For instance, agentic AI tools like Cursor and Claude Code help people plan and execute coding tasks. Two design choices shape the practical character and abilities of an agent. The first design choice is what the agent can reach, and whether it can create data as well as read it. The second is how much autonomy the agent has — whether it follows a defined procedure, plans its own steps, or requires human approval before acting. The rights questions raised by agentic AI follow from those design choices, and new and influential thinking on how agents should be governed is released every week.

Predictive analytics systems

Predictive analytics is another branch of AI and data science that has significant impacts on people's lives and rights. Predictive analytic systems are algorithms that use machine learning methods to analyse a dataset of examples, in ways that allow predictions to be made about new unseen examples. The *Algorithm Charter for Aotearoa New Zealand* describes a spectrum of longstanding statistical methods such as regression models, 'symbolic' methods such as decision trees and Bayesian inference, through to more complex systems such as neural networks.²² The focus of the Charter is on the uses of predictive analytics systems with a high risk of unintended consequences or significant impact if things go wrong, and on whether there is meaningful human oversight of decisions informed by algorithms.

AI and other digital technologies are part of a wider system

AI systems do not exist in isolation. They sit inside a wider technology system: an internet stack²³ (connectivity, cloud infrastructure, platforms); enabling software (operating systems, applications, AI models); connected sectors (the regulated domains in which AI is deployed — health, education, finance, justice); enabling hardware (smartphones, devices, chips, data centres, with their climate and mineral-extraction consequences); and associated technologies (biometrics, the internet of things, drones, wearables, smart glasses, brain-computer interfaces, with rapid convergence between them).

Decisions are made by humans and institutions at every level of technological systems. Humans make decisions about the way technology is designed, created, tested, put into operation, and later monitored and maintained over time. When human beings decide to use a technology for a particular purpose, they are making a choice, and they are responsible for the intended and unintended consequences of that choice. The MIT AI Risk Repository is a peer-reviewed meta-review of 74 AI-risk frameworks. It found that human decisions cause nearly as many AI risks as the AI systems themselves.²⁴ The te ao Māori concept of whakapapa can be applied to data and to an algorithmic system — tracing the history of the choices and data embedded in a system. This gives this point another working articulation.²⁵ Responsibility cannot be deflected onto technology. Various technological and academic disciplines now have a well-established approach to 'by design' protections related to ethics, human rights, and the law.²⁶

Introduction to New Zealand's human rights framework

This section of the report introduces New Zealand's human rights framework and explains how a human rights-based approach can be applied to AI and digital technologies. It aims to build understanding and provide a conceptual grounding for the remainder of the report.

Aotearoa New Zealand already has a human rights framework

Te Tiriti o Waitangi, international human rights instruments that bind Aotearoa New Zealand, and New Zealand law which gives partial effect to the binding international instruments, together supply a durable, non-partisan basis for naming what is at stake and for setting the limits within which choices can be made. Collectively these instruments and their application form a human rights framework for Aotearoa New Zealand (the framework). They provide a conceptual structure for identifying, evaluating, and addressing the rights at stake in any AI or digital system. It is a framework in the sense that it provides a way of thinking and a methodological approach, not in the sense of a single document or operational instrument.

These foundations do not have to be invented for AI and other digital technologies, they just have to be applied consistently. Many actors have a role in this, and the core rights and obligations covered by the framework are a matter of law, and do not depend on the agreement of a particular stakeholder. Together, Aotearoa New Zealand's human rights framework gives the country a reference point that is settled at its foundation and dynamic in its application, capable of responding to new technology, new institutional configurations, and new harms as they emerge.

Te Tiriti o Waitangi

Te Tiriti o Waitangi is Aotearoa New Zealand's founding constitutional and human rights document. Its text aligns with core human rights principles subsequently enshrined in the international instruments discussed further below — including the three instruments that comprise the International Bill of Human Rights and the UN Declaration on the Rights of Indigenous Peoples (UNDRIP). International human rights law reinforces Te Tiriti in the Aotearoa New Zealand context.

Te Tiriti o Waitangi contains constitutional, civil, political and territorial rights protections for hapū Māori. Both The Waitangi Tribunal²⁷ and the High Court²⁸ confirm that public powers affecting Māori must be exercised in line with Te Tiriti o Waitangi, even when this is not explicitly stated in legislation.

New Zealand's legislative frameworks

Domestically, the New Zealand Bill of Rights Act 1990 (BORA) enshrines some of the civil and political rights contained in the International Covenant on Civil and Political Rights (ICCPR) into our domestic law. The Human Rights Act 1993 is Aotearoa New Zealand's primary anti-discrimination legislation. It promotes and protects human rights by prohibiting unlawful discrimination and provides the mandate for the already established Te Kāhui Tika Tangata Human Rights Commission to promote and protect the full scope of human rights. The Privacy Act 2020 forms a key part of Aotearoa New Zealand's human rights framework by protecting individuals' rights

to privacy alongside other human rights and establishing principles governing the collection, use, and disclosure of personal information.²⁹ The Privacy Act 2020 operates a binding, code making power the Privacy Commissioner has already exercised over biometrics. A guide to responsible AI for businesses from the Ministry for Business, Innovation and Employment lists other statutes which apply.³⁰

International human rights frameworks

Currently, there is no international law which focuses specifically on AI, or automated decision-making, although there are several countries calling for such an agreement.³¹ However, international human rights provide a well-developed and settled framework which can apply to changing circumstances, including technological developments.³² These apply both online and offline.³³

The International Bill of Human Rights refers to the core set of international instruments that collectively articulate the fundamental rights and freedoms to which all people are entitled. It comprises three key documents:

- the Universal Declaration of Human Rights (UDHR),³⁴ adopted in 1948 as the international foundation of human rights,
- the International Covenant on Civil and Political Rights (ICCPR),³⁵ and
- the International Covenant on Economic, Social and Cultural Rights (ICESCR).³⁶

The latter two instruments were both adopted in 1966 and are legally binding on States that ratify them, which includes Aotearoa New Zealand, even if the specific rights contained within them are not currently incorporated into domestic law. Together, these three instruments contain the full spectrum of rights necessary for every person to live a life of dignity forming the foundation of modern international human rights law and guiding states in their obligations to respect, protect, and fulfil human rights globally.

Beyond the International Bill of Human Rights, there are seven other core human rights treaties³⁷ which address specific areas of protection and equality. These include the five ratified by Aotearoa New Zealand:

- the Convention on the Elimination of All Forms of Racial Discrimination (CERD),³⁸ combatting racial discrimination,
- the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW),³⁹ advancing gender equality,
- the Convention Against Torture and other Cruel, Inhuman and Degrading Treatment or Punishment (CAT),⁴⁰ prohibiting torture and ill-treatment,
- the Convention on the Rights of the Child (CRC),⁴¹ safeguarding children's rights to survival, development, and participation, and
- more recent instruments like the Convention on the Rights of Persons with Disabilities (CRPD),⁴² promoting inclusion and accessibility.

Together, these treaties complement the universal framework set out in the International Bill of Human Rights by addressing vulnerabilities and ensuring that human rights protections extend to all groups and contexts.

Some countries belong to regional human rights systems which have their own treaties or regional human rights standards and/or a regional body which also issues statements on human rights. For example, European countries have the Council of Europe's *European Convention on Human Rights*⁴³ and the European Union's *Declaration on Digital Rights and Principles* (2022)⁴⁴. As there is no regional human rights system in the Asia-Pacific region, Aotearoa New Zealand is mainly guided by international human rights law that comes from United Nations treaties and other international sources.⁴⁵

The binding, international human rights obligations described above must also be understood against the backdrop of the UN Declaration on the Rights of Indigenous Peoples (UNDRIP). Although not a treaty, UNDRIP is the most comprehensive and authoritative international human rights instrument dealing with the rights of Indigenous peoples.⁴⁶ UNDRIP relates to technology and AI by providing a human rights framework that applies to digital systems which affect Indigenous peoples, requiring that AI systems respect self-determination, indigenous authority over data and knowledge, are non-discriminatory, and there is free, prior and informed consent when using data.

Te Pou Matakana Limited v Attorney-General⁴⁷

Te Pou Matakana Limited v Attorney-General is the High Court decision that confirms Te Tiriti o Waitangi binds the exercise of statutory power even where the governing statute carries no express Tiriti clause. The case concerned the Privacy Commissioner's response to a request by the Whānau Ora Commissioning Agency for Ministry of Health data to support Māori COVID-19 vaccination outreach. The Court found that the Privacy Commissioner, in exercising statutory powers under the Privacy Act, was required to act consistently with Te Tiriti.

Implementing a human rights-based approach

Aotearoa New Zealand's human rights framework provides clear standards on *what* is required to uphold human rights. These are the human rights treaties and laws themselves which set out the rights to be protected. A human rights-based approach (HRBA) helps to clarify *how* to apply these standards. It provides principles for translating the standards into decision-making in order to advance human rights. In practice, a HRBA involves identifying which rights are at stake, analysing impacts on different groups, assessing whether any limitations are lawful and proportionate, and ensuring decisions are evidence-based and use the least rights-restrictive option. It focuses on addressing underlying systemic causes, not just symptoms, and requires strong safeguards such as transparency, independent oversight, and accessible avenues for redress.⁴⁸

A HRBA rests on broad principles of participation, accountability and transparency, non-discrimination and equality, empowerment, and legality. PANEL is the acronym used to describe these principles. The description of a HRBA detailed in the table below includes a Te Tiriti-based approach, which sits in the broader framework of human rights.

Using a HRBA requires embedding these principles at every stage of the technology’s life cycle, from design to deployment. This means that AI and other digital technology systems should be conceived and implemented with the explicit purpose of respecting, protecting, and promoting human rights.⁴⁹ This is referred to as a ‘human rights by design approach’.⁵⁰ Such a rights-based approach requires systematic assessment, transparency, accountability mechanisms, and the inclusion of stakeholders — especially impacted communities and minorities — in governance and decision-making processes.⁵¹ This approach has been affirmed by the UN General Assembly.⁵²

Below is a summary of the HRBA drawn from international literature, as it applies to AI and digital technologies.⁵³ What applying a HRBA to AI and digital technologies looks like in practice will vary depending where a given entity falls within the ‘chain’. For example, what is required from a developer may be different from what is required from a government ministry using a new tool.

Table 1: Human Rights-Based Approach principles and their application to AI and digital technologies in the Aotearoa New Zealand context

Principle	Description and how it applies to AI and digital technologies
Participation	Participation is about ensuring people affected by decisions are actively, freely, and meaningfully involved in shaping the decisions that impact their lives, with particular attention to those who are most marginalised. Participation must be early on and continuous (rather than retrospective), have real influence over decisions (not symbolic or consultative only) and importantly the public must have access to clear and accessible information, and resources to participate effectively. In terms of Te Tiriti obligations, as a Tiriti partner the government has an obligation which goes beyond consultation. As a partner, Tangata Whenua must have meaningful influence over how AI used within the public sector is governed, deployed, and challenged. This includes using approaches which align with Te Tiriti o Waitangi, Māori data sovereignty, and indigenous rights frameworks.

Accountability and Transparency	These principles require that duty-bearers are answerable for their decisions and actions that affect human rights, and that these processes, decisions, and outcomes are open, clear, and accessible so people can understand them and seek redress where rights are not upheld. There must be effective remedies provided (judicial/administrative, company-level grievance) where harms occur. See the ‘right to remedy’ below. The concepts in these principles are interconnected: transparency enables accountability and accountability gives transparency meaning. In terms of AI, transparency and accountability are of concern given how these systems are developed by the private sector and are ‘black boxes’, meaning we can see the input and the output, but not clearly how or why the system arrived at its decision.⁵⁴ For AI and digital technology, transparency requires that systems are not obscure, secret, or inscrutable to the people affected by them. In practical terms, this means:⁵⁵ • people should know when an AI system is involved in a decision affecting them, • meaningful information should be available about how the system operates, • risks and impacts should be assessed and disclosed where appropriate, and • AI systems should not be so opaque that scrutiny becomes impossible. Importantly, transparency under a HRBA does not require full disclosure of source code to the public, but it does require explanations that are accessible and understandable by non-experts.⁵⁶ Transparency is especially important in relation to government use where AI informs or makes decisions that impact human rights (such as welfare, health, immigration, policing). The public must have access to information about why AI is being introduced, the problem it is meant to solve, why AI⁵⁷ (rather than non-automated approaches), who decided to use it, and how data is being used. In terms of accountability, the use of AI requires an identifiable human decision-maker, clear legal and ethical responsibility, organisational ownership of outcomes, and a clear allocation of responsibility, such that accountability is not displaced onto the technology itself.⁵⁸
--	---

	The UN Office of the High Commissioner for Human Rights has recommended the following actions to ensure practical accountability:⁵⁹ • human rights due diligence throughout the entire AI lifecycle, • impact assessments before deployment, • effective oversight mechanisms, • remedies for people harmed by AI systems, and • restrictions or bans on AI applications that cannot be operated consistently with human rights law.
Non-discrimination and Equality	Non-discrimination means that all people can enjoy their human rights equally in law and in practice, without exclusion or disadvantage on the basis of prohibited grounds. It requires taking positive steps to address systemic inequalities affecting marginalised groups. In Aotearoa New Zealand this includes Māori, Pacific communities, women, ethnic and religious minorities, disabled people and the Rainbow community. Equality is recognising that everyone is entitled to the same rights and dignity, while taking proactive steps to address inequalities and remove barriers so that people can enjoy those rights in practice on an equal footing. In a HRBA, applying the non-discrimination principle is not just about avoiding biased outcomes. It requires active, ongoing steps to ensure AI systems do not create, reinforce, or legitimise direct, indirect, or structural discrimination across their entire lifecycle. AI systems as they are currently designed have inherent bias — this is a technical feature due to the data they use.⁶⁰ This makes measuring and monitoring bias even more important, particularly because those most impacted by the system are least likely to be well positioned or resourced to be able to do that themselves. Measuring and monitoring bias ensure digital systems do not reproduce or deepen existing biases, or work better for some groups and not others. An example of what this might look like in practice is testing hiring, welfare, education, and policing tools to understand if there are disparate impacts on women, disabled people, ethnic minorities, Indigenous peoples, and other groups facing structural disadvantage. It also means designing technology to be accessible and inclusive from the outset, using representative data, consulting affected communities, and monitoring outcomes over time.

Empowerment	Empowerment means that everyone is entitled to claim and exercise their rights and freedoms. Individuals and communities need to be able to understand their rights and participate fully in the development of policy and practices which affect their lives. This is closely linked with the participation outlined above. Empowerment is about ensuring people are able to understand, influence, challenge, and shape the AI and digital systems that affect their rights and lives. It goes beyond transparency and accountability by focusing on people’s agency, capability, and participation. An example of empowerment is engaging rights-holders, for example, Māori, disabled people, children, in the design, testing, and evaluation of AI systems so they can influence how the technology operates and how risks are managed. This is empowerment because people help shape decisions that affect them, rather than simply being informed about them.
Legality	Legality means that all laws, policies and decisions are grounded in, and consistent with, domestic and international human rights law, and that any restriction on rights is authorised by law and subject to rule-of-law safeguards.⁶¹ Actions must have a basis in and comply with domestic law, however domestic law itself should be consistent with international human rights obligations and standards. The HRBA is explicitly grounded in international human rights law.⁶² In Aotearoa New Zealand, section 5 of BORA provides that the rights and freedoms affirmed in the BORA may be subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society. This principle requires that AI development, use and governance be in line with domestic law and binding international human rights norms, not merely ethics guidelines. Any restrictions on rights (for example content moderation or surveillance) must be proportionate, lawful, pursue a legitimate aim, and be necessary and proportionate.

Indigenous rights and Māori data sovereignty

Indigenous rights

In the Aotearoa New Zealand context, a HBRA to AI and digital technologies engages a range of rights relevant to Māori as indigenous peoples, as articulated in UNDRIP and Te Tiriti o Waitangi. Importantly, UNDRIP⁶³ includes Indigenous Peoples' right to self-determination.⁶⁴ Further, the articulation of Indigenous rights in UNDRIP, which Aotearoa New Zealand endorsed in 2010, provides the internationally accepted minimum standards for the survival, dignity and well-being of Indigenous peoples.⁶⁵ These rights relating to AI and digital technologies include, but are not limited to, the following:

- the right to be free from discrimination, which could potentially be engaged when accessing digital services or during the design of AI systems used in public services, which produce unequal outcomes for Māori.
- the right to have their histories, languages, oral traditions, philosophies, writing systems and literatures protected,
- the right to participate in decision making impacting them or their rights,
- the environmental impact of extensive energy consumption, greenhouse gas emissions and water use associated with AI have the potential to adversely impact the rights of Māori "to conservation and protection of the environment and the productive capacity of their lands or territories and resources"⁶⁶

In addition, the right to health (outlined below) could be engaged for Māori when the tools deployed are trained on datasets that do not adequately represent Māori and Pacific peoples.⁶⁷

Māori intellectual property and data sovereignty

In Aotearoa New Zealand, an area that has received considerable attention for good reason is the impact of AI and other digital technologies on the intellectual property rights of Māori.⁶⁸ There is a rich tradition of indigenous leadership in articulating intellectual property rights which predates the advent of new digital technologies. Aotearoa New Zealand hosted the First International Conference on the Cultural and Intellectual Property Rights of Indigenous Peoples in Whakatane, leading to the Mataatua Declaration on Cultural and Intellectual Property Rights of Indigenous Peoples (1993).⁶⁹

Māori intellectual property is subject to the rights articulated in Te Tiriti o Waitangi and UNDRIP. For example, Māori data is subject to the rights articulated in the UNDRIP, Article 19 (free, prior and informed consent) and Article 31 (control over cultural heritage and traditional knowledge).⁷⁰ In addition, Māori data is protected through Te Tiriti o Waitangi. Tino rangatiratanga under Article 2 is the protected interest at stake: authority and self-determination over taonga, of which data is one expression. The commission also notes the High Court's confirmation in *Te Pou Matakana Limited v Attorney-General* [2021] NZHC 3319⁷¹ that a public body exercising statutory powers (there, under the Privacy Act) must do so in accordance with Te Tiriti and its principles.

The commission heard during the development of this report that, to Māori, data is a taonga — a position supported by the Waitangi Tribunal in its *Ko Aotearoa Tēnei* report.⁷² This also reflects that Mātauranga Māori is taonga. Data is an expression of mātauranga, and the systems built on it carry the same status. Control over that data is a Tiriti obligation.

Te Mana Raraunga, the Māori Data Sovereignty Network, provides the following definition for Māori data:⁷³

“Māori data are data that are produced by Māori, and data that are about Māori and the environments we have relationships with. Data are living tāonga and are of strategic value to Māori. Māori data include but are not limited to:

- data from government agencies, organisations and/or businesses
- data about Māori that are used to describe or compare Māori collectives
- data about Te Ao Māori that emerges from research.”

Māori data requires special protections when it is collected, used and shared by government agencies. Te Kāhui Raraunga was established in 2019 to lead action required to realise the advocacy of the Data Iwi Leaders Group (Data ILG), a leadership group under Pou Tangata, a Pou of the National Iwi Chairs Forum. While Te Kāhui Raraunga does not claim a mandate that displaces iwi or hapū as rights holders, it does enjoy the substantial and ongoing support of the composite iwi members of the National Iwi Chairs Forum. In 2023, Te Kāhui Raraunga published the *Māori Data Governance Model*,⁷⁴ which outlines Māori data governance values, Māori data security considerations, and a set of best practices to inform ethical advice for the treatment of all data, including Māori data. It is comprehensive, articulates advanced thought leadership and robust analysis of Indigenous and Tiriti rights impact, and provides guidance for the public sector to support Tiriti-aligned approaches to Māori data governance.

Māori data sovereignty is described by Te Mana Raraunga as follows:⁷⁵ “Māori Data Sovereignty recognises that Māori data should be subject to Māori governance. Māori data sovereignty supports tribal sovereignty and the realisation of Māori and Iwi aspirations.”

In 2025, Te Kāhui Raraunga published *Māori AI Governance: A Framework for Ethical Governance of AI in Aotearoa*. It outlines the following principles to develop how Māori data sovereignty must extend to AI systems:⁷⁶

- Free, Prior and Informed Consent (FPIC) for all Māori data use,
- Recognition of collective privacy rights beyond individual privacy protections,
- Māori authority over data regardless of storage location or AI processing jurisdiction, and
- Prohibition of generative AI tools built on Māori data without Māori involvement.

Te Mana Raraunga principles⁷⁷ and Te Kāhui Raraunga’s AI governance framework are anchored in the 2018 international CARE Principles for Indigenous Data Governance: Collective Benefit, Authority to Control, Responsibility and Ethics.⁷⁸

The commission strongly supports Māori data sovereignty as a foundational principle, not a supplementary one, grounded in rights affirmed under Te Tiriti o Waitangi and in international human rights law. It sits inside the mutually reinforcing Te Tiriti and human rights framework presented in this report. We have emphasised the work of Te Kāhui Raraunga in the report, as the National Iwi Chair's forum's representative voice, therefore enjoying the support of this wider group of collective rights holders with regards to data sovereignty matters.

These rights are constitutional in nature and enduring in their application. At the same time, the commission recognises that how Māori data sovereignty is given practical effect will necessarily vary depending on context. The principle itself is not in question; rather, it is the design of governance arrangements that must be responsive to different settings, uses, and relationships. Accordingly, the frameworks that operationalise Māori data sovereignty will not be uniform, but must be capable of adapting while remaining anchored in these underlying rights.

The commission also heard from contributors with deep expertise in Māori data governance that an effective downstream framework depends on first classifying data according to its sensitivity. This step should precede decisions about consent, access, or use. Such an approach allows governance requirements to scale proportionately with both the level of risk and the nature of the system, rather than applying a uniform and potentially impractical standard across all data. For example, a clinical decision-support tool drawing on identifiable Māori patient data will engage materially different obligations than a public-facing system trained on openly available content that includes te reo Māori.

Waikato-Maniapoto voice model — conditional licensing in practice

An iwi-led research project based out of Waikato University built a reo Māori synthetic voice in the Waikato-Maniapoto dialect. A commercial company approached the team about a licensed use of the voice: it held government contracts to produce mathematics resources for years 1–10, already translated into te reo Māori, and now needed the resources to be spoken aloud. This request required careful consideration because the model was based on a specific person's voice which was provided to the project for iwi benefit not commercial gain. The voice usage was agreed, on specific terms. The licence was limited to use for mathematics resources. Payment was agreed for access, with a proportion of funds to flow back to the speakers whose voices made the model possible. Tamariki now have the chance to learn maths in te reo Māori, in a voice that sounds like someone from their community and is in their dialect. The case demonstrates that sovereignty includes refusal and includes the power to set terms. A regime that draws hard lines against any commercial engagement with Māori-language models may produce neither protection nor empowerment. Instead, tino rangatiratanga might mean saying: if you are doing this, here is how you do it properly, with consent, with limits, with funds returned, with accountability. It is for iwi and hapū to decide which approach will be more likely to be supported, more likely to produce wider beneficial outcomes, and more likely to improve the implementation of mana motuhake through Māori data sovereignty.⁷⁹

Te Mana Raraunga Māori Data Sovereignty Principles,⁸⁰ Te Kāhui Raraunga Māori Data Governance Model,⁸¹ and the AI Governance Framework,⁸² the body of work led Māori academic and industry experts (including the 2025 State of the Nation report on implementation across central and local government,⁸³ the six Tiriti-based AI ethical principles,⁸⁴ and the WAI 2252 four-step framework⁸⁵), and the operational frameworks developed in commercial and infrastructural settings are illustrative of the wealth of work in this area already being led by Māori.

A wider point also follows. Te Kāhui Raraunga has argued that addressing Māori data sovereignty addresses data sovereignty for everyone in Aotearoa New Zealand. It considers the questions about jurisdictional control, collective rights, and the relationship between data and the people are not Māori-specific in their reach, even where Te Tiriti gives them their constitutional source. The question of how communities can exert meaningful control over information about them is a universal concern and only growing in significance. Māori sovereignty practices can serve as a model that broader sovereignty processes in Aotearoa New Zealand could emulate.

Pacific data sovereignty

Inspired in part by Te Mana Raraunga and the Global Indigenous Data Alliance, the Pacific Data Sovereignty Trust was founded in 2021 to address gaps in how Pacific communities are represented in national data. As noted on their website, they are “guided by the principle that ‘data is the new land’”, and “ensuring that nothing about Pacific peoples is done without Pacific peoples”.⁸⁶ The Trust advocates for Pacific data to be understood as taonga and that Pacific peoples should lead its interpretation and use. In the age of AI, the Trust plays an important role championing the rights of Pacific communities to retain control of their information and stories.

The human rights risks and opportunities of AI and digital technologies

As noted in the introduction, AI and other digital technologies offer significant opportunities to protect and promote human rights in Aotearoa New Zealand, from improving accessibility for disabled people to enabling community-led projects. With those opportunities come risks, which are also real, and in some cases already impacting people's rights and wellbeing.

This section discusses some of the key rights that are engaged by AI and digital technologies and the risks to people and communities if these tools and technologies are used in ways that do not align with human rights. It also outlines the opportunities and existing benefits offered by AI and digital technologies, in order to understand what Aotearoa New Zealand might stand to gain by developing and deploying these technologies in rights-enhancing ways.

Key human rights engaged and the attendant risks

The section below provides an overview of some of the key human rights engaged by AI and other digital technologies, and the associated human rights risks and considerations. We note that, given the cross-cutting nature of these technologies, many more rights are engaged through AI's development and use than can be covered in this report.

All human rights are interdependent and interconnected, so there is crossover between rights in many cases — each deployment of AI or digital technology usually engages several rights at once. For example, a facial recognition system installed in a public space engages privacy, equality, freedom of expression (through the chilling effect on assembly), and the right to participate in public affairs. A human rights framework provides a structured method of identifying all relevant rights concerned, as well as clear expectations on how they should be addressed.

Understanding the rights engaged by a use of AI or digital technology and the attendant risks is important in order to avoid blind spots in how technology is built, used, and regulated. However, it is also important to recognise that properly identifying these risks and understanding their impacts for a specific application requires the participation of the people affected. Companies and governments are likely to miss these impacts unless people are meaningfully involved.

The human rights discussed in this section are drawn from the International Bill of Human Rights, the five other core international human rights treaties Aotearoa New Zealand has ratified⁸⁷ and have binding effect, the UNDRIP, and the developed reasoning of the UN treaty bodies in their General Comments.⁸⁸ This section is also informed by the work of the UN B-Tech Project⁸⁹ (the project run by the UN Office of the High Commissioner for Human Rights to apply the UN Guiding Principles on Business and Human Rights to digital technology), the OHCHR Mapping Report⁹⁰ and the International AI Safety Report 2026.⁹¹

Right to privacy⁹²

While the right to privacy under international human rights law is not absolute, any instance of interference must be provided by law and subject to a careful and critical assessment of its necessity and proportionality.

In Aotearoa New Zealand, the BORA does not include a free-standing right to privacy. The Privacy Act 2020 carries practical protection, supported by the common-law tort recognised in *Hosking v Runting*,⁹³ but the absence of a constitutional right is itself a structural feature the framework asks the State to address.⁹⁴

Considerations and risks: AI systems collect, process, and share personal data at scale, raising concerns over transparency, profiling, biased decision making, misuse, retention, and data sovereignty. Training data can be scraped without consent, sensitive inputs stored and reused, and surveillance made cheaper and larger in scale. The collective dimension of privacy is engaged by population-level profiling and by inference about groups, and often AI systems have been found to be designed to maximise comprehensive data collection in a way inconsistent with the right to privacy. AI systems can be used for the production of non-consensual intimate imagery like sexual deepfakes.

The ICCPR protects against arbitrary or unlawful interference with privacy and unlawful attacks on honour and reputation which is central to control over intimate decisions and the use or misuse of one's image or personal information.

Māori data governance in practice

Foodstuffs South Island (FSSI) piloted live facial recognition in its supermarkets and then built a Māori data governance overlay on top of the general law. The regulatory floor was already set: after the Privacy Commissioner's inquiry into a parallel Foodstuffs North Island trial,⁹⁵ the Biometric Processing Privacy Code 2025 imposed thirteen biometric-specific rules on all agencies.⁹⁶ Rather than treat that floor as sufficient, FSSI voluntarily engaged Te Kāhui Raraunga and applied its eight-pou Māori Data Governance Model — a public-sector framework — to a private-sector deployment, shaping watchlist enrolment and a tikanga-aligned response to misidentification.⁹⁷

This example demonstrates that Māori data governance approaches are being applied in the private sector in Aotearoa New Zealand.

International treaties/sources:⁹⁸ Article 12 of UDHR; Article 17 of ICCPR; UN Human Rights Committee General Comment No. 16; Article 16 Convention on the Rights of the Child.

Right to enjoy the benefits of scientific progress and its applications⁹⁹

The right to access to, to participate in, and to enjoy science and its benefits covers all sciences: life, natural, physical, behavioural and social sciences. It also includes the multiple fields of application of scientific knowledge, such as engineering, technologies and health.

The Committee on Economic, Social and Cultural Rights' General Comment 25 elaborates on the specifics of the right, which has five elements.¹⁰⁰ The right requires availability of scientific knowledge and institutions, accessibility without discrimination, quality of science and education, and acceptability, meaning scientific activity must be conducted ethically and with respect for human rights. The right also includes the freedom of scientific research, requiring protection of scientific inquiry, expression and collaboration including international cooperation, alongside public participation in, and access to, the benefits of science.

As a core obligation, states must develop a participatory national framework law around the right to the benefits of scientific progress that includes legal remedies in case of violations.¹⁰¹ States must also adopt and implement a participatory national strategy or action plan for the realisation of this right that includes a strategy for the conservation, the development and the diffusion of science.¹⁰²

The Committee has also highlighted the need to take a holistic, inclusive human rights approach to the use of all technologies when making decisions about their development and use.¹⁰³ This includes establishing a legal framework that imposes due diligence requirements on non-state actors especially in the context of big technology companies, reviewing companies to prevent discrimination at both the input and output levels of artificial intelligence systems and other technologies, and preventing the exploitation of data by regulating ownership and control of data according to human rights principles.¹⁰⁴

While the right is not expressly recognised as a standalone right in domestic law, Aotearoa New Zealand has committed to uphold it through its ratification of the ICESCR.¹⁰⁵

Considerations and risks: Digital exclusion, including due to lack of access to technologies and/or a stable internet connection, poses a threat to this right and further exacerbates inequalities around access to education, healthcare, work and other areas. In the context of AI, this right means that states must ensure that new technologies support, rather than undermine, the enjoyment of economic, social, and cultural rights. Examples include access to education, health care, and social protection through AI enabled services. At the same time, states must establish mechanisms for accountability, ensuring individuals can contest algorithmic decisions that affect their rights.¹⁰⁶

AlphaFold, Gemini, and Shane Legg — the right to share in scientific progress¹⁰⁷

DeepMind's AlphaFold has predicted the three-dimensional structure of nearly every protein known to science, accelerating biomedical research that would otherwise have required decades of laboratory work. Its co-creators were awarded the 2024 Nobel Prize in Chemistry. DeepMind's co-founder and chief scientist Shane Legg is a New Zealander. The Gemini family of models, also developed at Google DeepMind, has put multimodal AI in the hands of millions of people worldwide, supporting access to information across language, image, and audio. The right to enjoy the benefits of scientific progress and its applications, recognised at Article 15(1)(b) of ICESCR and developed by CESCR General Comment Number 25, is engaged by these systems. The framework's duty to fulfil is the side of the test that asks not only whether harms are prevented but whether benefits are reaching people.

The German Sovereign Tech Fund¹⁰⁸

Germany established the Sovereign Tech Fund in 2022 to provide public investment in the open-source software and infrastructure that underpins the country's digital economy. Critical open-source components — cryptographic libraries, package managers, security toolchains — are often maintained by very small numbers of unpaid contributors, despite being relied on by millions of services. The Fund identifies critical components, provides multi-year funding, and treats their maintenance as a public good. The German design is conscious of three things. First, the country's economic and security position depends on infrastructure it does not own. Second, open-source components are systemic risks when they are under-maintained — the Log4Shell vulnerability in 2021 was a recent reminder.¹⁰⁹ Finally, public investment in the maintenance of common goods is itself a rights-respecting policy because it strengthens the infrastructure on which rights depend.

International treaties/sources: Article 27 of UDHR; Article 15(b) of ICESCR; Committee on Economic, Social and Cultural Rights General Comment 25.

Right to freedom of expression and access to information¹¹⁰

The right to freedom of expression has three parts:

- the right to hold opinions without interference (freedom of opinion),
- the right to seek and receive information (access to information), and
- the right to impart information (freedom of expression).

Unlike the right to freedom of opinion, the rights to express and access information and ideas may be subject to restrictions under limited circumstances.¹¹¹

The right to freedom of expression is protected under section 14 of the New Zealand BORA¹¹²

The UN Human Rights Committee, which monitors state compliance with the ICCPR has concluded that the right to freedom of opinion requires freedom from undue coercion in the development of an individual's beliefs, ideologies, reactions and positions.¹¹³

AI systems also have an impact on the information ecosystem, generating more content and false information which in turn makes access to reliable, correct information much harder for individuals to achieve.¹¹⁴

Considerations and risks: Algorithmic systems that invisibly rank, filter, or personalise information can interfere with this right if they are opaque or biased.¹¹⁵ The dominance of particular modes of AI-assisted curation and high rate of inaccuracies raises concern about the systems impact on the capacity of the individual to form and develop opinions. Equally, managing the scale of online content may be impossible to manage without the use of automated systems. This also impacts the right to political participation.¹¹⁶ AI systems can also be used to monitor speech at scale through surveillance and content removals.

Deepfakes, satire, and political cartoons

A long democratic tradition treats caricature and parody of political figures as essential expression. AI-generated imagery and video extend that tradition with new capability — and new ambiguity. A deepfake video of a serving politician saying something they never said can be devastating satire, devastating defamation, or actionable election interference, depending on context, framing, and the audience's ability to read the signals. For Māori, deepfakes might include tapu features, such as tā moko. Existing law has tools — defamation, the Electoral Act, the Harmful Digital Communications Act, contempt of Parliament — but the tools were designed for a world in which faking video took resources only states and well-funded studios had. A human rights approach helps to evaluate these trade-offs. In practice, many of the restrictions applied against AI-generated videos, audio and images result from the policies applied by private technology companies. Some of these explicitly adopt a human rights framework, but often their judgements are difficult to test or independently review, and may lack legitimacy.¹¹⁷ Restrictions on AI-generated political imagery must pass the proportionality test: a law that captured legitimate satire would be a serious limitation on expression, on assembly, and on the right to participate in public affairs. And the protective regimes the framework recommends for non-consensual sexual deepfakes and election-targeted fabrications need to be designed in a way that does not foreclose the long, valuable tradition of irreverence about people in power. It should also be noted that AI is notoriously bad at spotting satire.¹¹⁸

International treaties/sources: Article 19 UDHR; Article 19 ICCPR; UN Human Rights Committee General Comment 34; Article 17 UNCROC (Right to Access Information); Article 21 Convention on the Rights of Persons with Disabilities (CRPD); Article 5 (d)(viii) International Convention on the Elimination of All Forms of Racial Discrimination (CERD); Article 16 UNDRIP; UN Joint Declaration (2025) on AI and freedom of expression.

Right to non-discrimination

Equality and non-discrimination are foundational principles of international human rights law that require all individuals to enjoy rights and equal protection of the law without unjustified distinction.¹¹⁹ Non-discrimination exists as both a standalone right in some treaties and as cross-cutting obligations that shape the interpretation, application, and enforcement of all human rights.

The right to freedom from discrimination is protected in Aotearoa New Zealand through section 19 of the BORA, which affirms the right to be free from discrimination on the grounds set out in the Human Rights Act 1993.¹²⁰ The Human Rights Act gives effect to that protection by prohibiting unlawful discrimination in areas such as employment, education, housing, and access to goods and services, and providing mechanisms for complaints and remedies.¹²¹

Considerations and risks: Increasingly AI systems mediate access to opportunities, services, information, and public power in areas such as employment, policing, migration, social protection, education, and online expression. AI tools and algorithms can perpetuate systemic bias and disadvantage especially in relation to minority groups.

International treaties/sources: Article 2 UDHR; Article 2 (1) ICCPR (in relation to rights in the Convention); Article 26 ICCPR (standalone right, equality under the law); Article 2 (2) ICESCR (in relation to rights in the Convention); Article 1 & 5 CERD (Racial Equality); Article 2 UNCROC (in relation to rights in the Convention); Article 1-2 Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW); Article 5 CRPD; Article 2 UNDRIP (see below).

Robodebt and the Netherlands childcare benefits scandal

Two of the most prominent national scandals of the past decade involving devastating human rights impacts on vulnerable people used AI in different ways, and neither of them used more modern “generative AI” systems that most people think about when they hear “AI” today.

Robodebt was the Australian Government’s automated debt-recovery scheme, operating between 2015 and 2019. It used income-averaging — comparing a person’s reported income to data held by the Australian Taxation Office — to issue debt notices to welfare recipients. The income-averaging method was unlawful from the outset, as the Royal Commission’s 2023 final report confirmed. Over \$1.7 billion in debt notices were raised against around 433,000 people. Some recipients took their own lives. The Royal Commission found that senior public servants and ministers had ignored repeated legal advice that the method was wrong.¹²² The Australian Government has paid more than a billion dollars in refunds and compensation.¹²³ Public servants associated with the scheme were investigated for criminal wrongdoing, emphasising that the human assurance and governance mechanisms around the system were also important, as well as its technical characteristics.

Another kind of AI — “risk scoring” — was used in the Netherlands in what is known as the childcare benefits scandal — the toeslagenaffaire. This saw the Belastingdienst, the Dutch tax authority, use risk-scoring methods to flag families suspected of childcare-benefit fraud between 2013 and 2019.¹²⁴ Around 26,000 families were wrongly accused, required to repay tens of thousands of euros, and forced into financial collapse.¹²⁵ Families with dual nationality were disproportionately affected and more than a thousand children were separated from their parents and placed in care.¹²⁶ The Dutch Government fell in 2021 over the scandal.

Both systems produced rights-violating outcomes at population scale because the algorithm encoded a policy choice that no one with authority interrupted in time, and accountability mechanisms failed.

Right to health¹²⁷

Everyone has the right to enjoy the highest attainable standard of physical and mental health as laid out primarily in Article 12 of ICESCR. While the right is not expressly recognised as a standalone right in domestic law, Aotearoa New Zealand has committed to uphold it through its ratification of the ICESCR.

The right to health encompasses not just the absence of disease or infirmity but “complete physical, mental and social wellbeing”.¹²⁸ It includes access to both timely and appropriate healthcare as well as the underlying social and economic determinants of health, such as conditions of work and adequate food and shelter.¹²⁹

Considerations and risks: The use of AI and algorithms in healthcare (for example diagnostic tools, large language models) raise concerns around inaccuracy, bias, accountability, data misuse, and professional liability¹³⁰. Relatedly, the increasing use of digital systems for delivering healthcare and holding healthcare information can create cybersecurity risks, particularly where information systems are not governed effectively or adequately resourced.¹³¹ In addition, emerging research suggests that large language models may play a role in validating or amplifying psychotic delusions, particularly in users already vulnerable.¹³² AI can also be used to support medical interventions if the proper supervision and checks are in place by improving diagnostics (e.g., analysing scans for early disease detection), personalising treatment plans, automating administrative tasks, among other things.

Emerging literature also looks at AI as an upstream determinant of health because it shapes access to many of the social determinants that drive health outcomes, including healthcare, education, employment, housing, social services, justice and information. As AI becomes embedded within these systems, it may function as a “super social determinant of health”, with the capacity either to reduce health inequities through improved access and inclusion, or to exacerbate existing disparities through bias, exclusion and unequal distribution of technological benefits.¹³³

International treaties/sources: Article 25 UDHR; Article 12 ICESCR; Committee on Economic, Social and Cultural Rights General Comment 14; Article 5 (e) (iv) CERD; Article 11 (1) (f), 12 and 14 (2) (b) CEDAW; Article 24 UNCROC; Article 25 CRPD.

Right to education¹³⁴

The right to education as primarily recognised under ICESCR, guarantees free and compulsory primary education and equal access to secondary and higher education for all without discrimination. Education is both a human right in itself and an indispensable means of realising other human rights. Education must be available, accessible, acceptable, and adapted to the needs of students.¹³⁵

While the right is not expressly recognised as a standalone right in domestic law, Aotearoa New Zealand has committed to uphold it through its ratification of the ICESCR. However, key aspects of the right such as free enrolment and education are recognised in the Education and Training Act 2020.

Considerations and risks: As AI becomes increasingly integrated into education systems, the consequence of digital exclusion grows more severe. Without equitable, affordable, and sustainable access to internet and digital devices, many learners are at risk of being left further behind and not being able to exercise their right to

education.¹³⁶ AI may hinder access to education due to lack of accuracy, including providing incorrect or biased information from flawed training data which requires critical evaluation by students and educators. On the other hand, AI tools may support educators to plan, deliver, and evaluate effective learning and teaching, although the evidence of this is developing.¹³⁷

International treaties/sources: Article 26 UDHR; Article 13 ICESCR; UN Committee on Economic, Social and Cultural Rights General Comment 13; Article 28 & 29 UNCROC; Article 10 CEDAW; Article 24 CRPD; UNESCO Convention Against Discrimination in Education.¹³⁸

Right to work¹³⁹

The right to work is a fundamental human right to have the opportunity to earn a living through freely chosen work, encompassing fair pay and safe working conditions. Although the right to work does not constitute the absolute and unconditional right to obtain employment, it does require states to work toward achieving full employment.¹⁴⁰

The right to work is not expressly recognised as a standalone right in domestic law, but New Zealand has committed to uphold it through its ratification of the ICESCR, and some aspects of the right are protected through employment legislation and anti-discrimination law.¹⁴¹

Considerations and risks: The role of AI in the automation of jobs could pose a real threat to the right to work — it may prevent some people from accessing the labour market and lead to job loss in certain sectors. The right to work is closely linked to the right to an adequate standard of living.¹⁴² Job automation may bring about a range of challenges that governments will have to address to ensure an adequate standard of living. AI and new technologies can also increase productivity, including by automating routine tasks, freeing humans for strategic work and enhancing decision-making through powerful data analysis. Other potential risks include declining demand for early-career workers in AI-exposed occupations, replacement of creative workers with synthetic output, and exploitative conditions for data labellers. There are also risks to psychosocial working conditions for workers through workplace surveillance, work intensification, reduced job autonomy and concerns around privacy and data use.¹⁴³

International treaties/sources: Article 23 UDHR; Article 6, 7 & 8 of ICESCR; UN Committee for Economic, Social and Cultural Rights, General Comment 18 — right to work; UN Committee for Economic, Social and Cultural Rights, General Comment 23 — right to just and favourable work conditions; Article 8 of ICCPR; Article 5(e)(i) CERD; Article 11 (1)(a–d) and (2)(a), and Article 14(1) and (2)(e) CEDAW; Article 32(1) UNCROC; Article 27 CRPD.

Right to a healthy environment¹⁴⁴

The right to a clean, healthy and sustainable environment is a universal human right that guarantees, at a minimum, access to clean air, safe water, a safe climate and non-toxic environments in which to live, work, study and play; and healthy biodiversity and ecosystems.¹⁴⁵ This right is still being developed in international jurisprudence. While there is not a universally agreed definition of the right to a

healthy environment, the right is generally understood to include substantive elements (listed above) and procedural elements.¹⁴⁶ The procedural elements include access to information, the right to participate in decision-making, and access to justice and effective remedies, including the secure exercise of these rights free from reprisals and retaliation.¹⁴⁷

Realising the right to a healthy environment also requires international cooperation, solidarity and equity in environmental action, including resource mobilisation, as well as recognition of extraterritorial jurisdiction over human rights harms caused by environmental degradation.¹⁴⁸ Aotearoa New Zealand supported international recognition of the human right to a clean, healthy and sustainable environment, including through UN processes,¹⁴⁹ but the right is not currently recognised as a standalone right in Aotearoa New Zealand's domestic law.

Considerations and risks: The proliferating data centres that house AI's servers, GPUs, networking equipment, storage systems and power infrastructure contribute to large amounts of economic waste once replaced, retired or disposed of. They are large consumers of water¹⁵⁰ and rely on critical minerals and rare elements, which are often mined unsustainably. They also use massive amounts of electricity, spurring the emission of planet-warming greenhouse gases.¹⁵¹ AI and new digital technologies can also support the right by optimising energy use, improving climate modelling, enhancing conservation efforts, and making various industries more sustainable.¹⁵²

International treaties/sources: *UN Human Rights Council Resolution, the human right to a clean, healthy and sustainable environment, (8 October 2021); UN General Assembly Resolution, The human right to a clean, healthy and sustainable environment, A/RES/76/300 (28 July 2022).*

Right to a remedy¹⁵³

Under international law, the right to an effective remedy imposes three core obligations on states:

- **Accessibility:** individuals must be able to identify, challenge, and understand the interference/violation of their rights.
- **Effectiveness:** the remedy must be capable of ending ongoing violations,¹⁵⁴ providing redress, and preventing recurrence.
- **Enforceability:** must involve prompt, thorough and impartial investigation of alleged violations;¹⁵⁵ remedies must be decided by competent authorities and implemented in practice.

The right to an effective remedy for breaches of BORA is a fundamental principle of New Zealand law. This reflects the common law maxim *ubi jus ibi remedium* ("where there is a right, there is a remedy"), New Zealand's obligations under article 2(3) ICCPR, and the majority's reasoning in *Simpson v Attorney-General* (Baigent's Case), where the Court of Appeal confirmed that effective remedies must be available for breaches of BORA rights, establishing a key constitutional principle that rights require practical means of vindication.¹⁵⁶ The right to remedy is closely associated with the right to justice as is protected by section 27 of BORA.

Considerations and risks: AI has significant implications for the right to remedy. Firstly, as harms can be unknown, remedy rights become meaningless if individuals cannot detect that a violation has occurred. International bodies have repeatedly held that remedies must be “practical and effective, not theoretical or illusory”.¹⁵⁷ AI opacity risks making remedies illusory by design. In addition, accountability gaps due to delegation and outsourcing mean it can be hard to enforce a remedy.¹⁵⁸

A lack of remedy for AI-driven harms can itself constitute a separate human rights violation. On a practical level the use of AI and digital systems may assist in supporting justice to be administered in a more timely and efficient way.¹⁵⁹

Whisper trained on te reo Māori without consent¹⁶⁰

OpenAI’s Whisper is a widely deployed speech-recognition model. Whisper’s training corpus included te reo Māori material gathered from the open web, including iwi broadcasters and community sources, without the consent of the speakers or of the communities whose taonga those recordings represent. Once a foundation model is trained, individual contributions cannot meaningfully be removed — the language has been absorbed into a system that is now run, monetised, and governed by a foreign company. The case demonstrates how the architecture of modern AI defeats the assumption — built into much Aotearoa New Zealand privacy and copyright doctrine — that information can be withdrawn. It also demonstrates how a global system that aspires to be ‘good for everyone’ can take from communities the very thing it claims to share with them.

International treaties/sources: Article 8 UDHR; Article 2 (3) ICCPR; UN Human Rights Committee General Comment 31; Article 6 CERD; Article 14 CAT; Article 12 (4) & 13 CRPD.

The rights of the child

Children’s rights under international law are primarily set out in the United Nations Convention on the Rights of the Child (UNCROC),¹⁶¹ which recognises that all individuals under 18 are entitled to a broad range of civil, political, economic, social, and cultural rights. Key principles include the best interests of the child as a primary consideration in all actions affecting them, respect for the child’s views in matters affecting them, the rights to survival and development, and non-discrimination.

Children face the same risks as adults with amplified vulnerability, and the framework places a heightened duty on the State including to take a precautionary approach when it comes to potential harm when children are involved.¹⁶² The General Comment¹⁶³ cited below addresses AI, algorithms, profiling, and automated content systems directly.

International treaties/sources: Convention on the Rights of the Child, with General Comment No. 25 (2021) specifically on children’s rights in relation to the digital environment.

The rights of persons with disabilities

Under international law, the rights of disabled people are articulated in the CRPD, which affirms that disabled people are entitled to the full and equal enjoyment of all human rights and fundamental freedoms. The CRPD emphasises principles such as dignity, autonomy, non-discrimination, full participation and inclusion in society, and equality of opportunity. It guarantees rights across a wide range of areas, including accessibility, education, health, employment, justice, and independent living, and requires states to remove barriers and provide reasonable accommodation to ensure equality in practice.¹⁶⁴ The CRPD also highlights the importance of respecting individual decision-making and legal capacity.

AI both enables rights for disabled people (multimodal interfaces, captioning, navigation, assistive systems) and threatens them (inaccessible design, biometric systems that fail on certain bodies, surveillance that displaces consent). The tension between accessibility and privacy is itself a rights question the framework requires the State to address.

International treaties/sources: *Convention on the Rights of Persons with Disabilities.*

Indigenous rights

The implications of digital technologies on Indigenous rights has already been touched upon in the Indigenous Rights and Māori Data Sovereignty section above. UNDRIP applies directly to digital technologies because AI systems increasingly affect knowledge, land, data, language, decision-making, and governance.¹⁶⁵ UNDRIP relates to technology and AI by providing a human rights framework that applies to digital systems which affect Indigenous peoples. This framework requires that AI systems respect self-determination and enable indigenous authority over data and knowledge, are non-discriminatory, and that there is free, prior and informed consent when using data. UNDRIP supports indigenous participation not just as stakeholders in AI policy, but as decision-makers, governors, designers, and owners of digital systems.¹⁶⁶

Considerations and risks: AI and digital technologies are having, and will continue to have, multiple impacts on Indigenous peoples and their rights. Indigenous representatives themselves are articulating these with great clarity. Indigenous rights holders need to be engaged to design risk assessment tools that enable AI and digital technologies to be measured against those rights at both a governance and operational level, and weighed against the concurrent obligations both Te Tiriti and UNDRIP places on the government and the public and private sectors.

Generative AI and te reo Māori — the homogenisation problem

Generative AI systems trained on te reo Māori scraped from the internet do not simply use the language — they change it. The models flatten dialectal variation, strip cultural context, and tend toward what one EAG member described as sanitised colonised reo Māori with inherent biases.¹⁶⁷ As they explained, the beauty of te reo is that it carries multiple perspectives within its structure — different iwi, different dialects, different ways of expressing the same truth. A model optimised for fluency treats that richness as noise. Young Māori children learning te reo through AI-assisted tools absorb the language as the model produces it. Those children become future leaders and kaitiaki of the language,

and the reo they learn will shape the reo of generations after them. The affected communities have no standing to challenge what the model says, no complaint route, no relationship with the company behind it. The harm is collective and intergenerational.

International treaties/sources: *United Nations Declaration on the Rights of Indigenous Peoples; the right to self-determination under Article 1 of ICCPR and ICESCR.*

The ‘right to explanation’

The right to explanation is an emerging legal concept, heavily centred on AI and automated decision-making, which asserts that individuals should be given a clear, understandable, and actionable explanation for decisions that significantly affect them, such as loan denials, job applications, or administrative actions.¹⁶⁸ Because of their design, some AI systems do not allow a meaningful explanation of how they operate in the same way as a human decision would.

While the right to explanation is not yet universally enshrined as a foundational human right in traditional international law, it is increasingly recognised as essential for protecting human dignity, autonomy, and due process in the digital age. The basis for this is found in European legislation¹⁶⁹ around AI and data protection, which does not apply in Aotearoa New Zealand. However, it is still helpful to mention right to explanation as an emerging right, and one that is closely linked to the rights to remedy, access to information, to participate in decisions affecting one’s rights, and (where children are affected) from the rights of the child as developed in the Committee on Children’s Rights General Comment No. 25.

The right not to be subject to automated decision making¹⁷⁰ is another emerging right, especially in the European context.

The opportunities: how AI and digital technologies can promote and protect rights

If deployed responsibly, AI and digital technologies can be powerful tools for promoting and protecting human rights and Te Tiriti o Waitangi, empowering people and communities, and maximising the ability of people to live with dignity. The risks outlined above are real and must be addressed — but so are the benefits. Whether these technologies expand rights and opportunities or deepen existing inequities will depend on the choices we make today and our willingness to actively invest in approaches that place human rights, Te Tiriti o Waitangi, and public wellbeing at their centre.

For instance, digital tools and automation can be the difference between a rights-promoting service being provided or not being available at all. AI can be a powerful enabler of disability rights, and can empower communities to address issues themselves rather than waiting for funding or outside expertise. It can also incentivise digitisation efforts that have lingered for decades, with consequences for fundamental rights including cybersecurity and access to healthcare.

These are not hypothetical opportunities. There are already documented, tangible benefits that affect the daily lives of people in Aotearoa New Zealand. Any governance framework for AI must account for these existing benefits and consider the future opportunities.

A range of key opportunities is presented below. We note that every opportunity requires careful reflection, as the same technology can often pose risks if deployed without the necessary care.

Encryption, the internet, and the infrastructure of rights

Many aspects of the contemporary digital technology landscape have played a historically significant role in promoting human rights.

The internet itself is a significant expression of the right to seek, receive, and impart information.¹⁷¹ The UN Human Rights Council has affirmed that internet access is essential to the exercise of human rights.¹⁷² For communities that were previously excluded from public discourse due to geography, disability, language, or economic status, the internet has created pathways to information, expression, and organisation that did not exist previously. Video calling, as is enabled by the internet, has transformed access to healthcare, education, legal services, and family connection, with particular benefits for rural, disabled, and migrant communities.

Encryption protects the right to privacy¹⁷³ in ways that are technically robust in a manner that legal protections alone are not. End-to-end encrypted communications give journalists, human rights defenders, whistleblowers, and ordinary citizens the ability to communicate without state or corporate surveillance. The UN Special Rapporteur on freedom of expression has repeatedly affirmed that encryption and anonymity tools are essential to the exercise of expression and opinion in the digital age.¹⁷⁴

Social media, for all its documented harms, has enabled collective action, political accountability, and cultural expression at a scale previously inaccessible to communities without institutional power.¹⁷⁵

Multimodal AI: a transformation in human-computer interaction

The current generation of AI systems represents a step change in how people interact with computers. Large language models and multimodal AI systems — AI models that can understand, process, and generate multiple types of data including text, images, and audio¹⁷⁶ — allow people to communicate with machines using spoken, written, or signed language rather than through code, command lines, or structured interfaces designed for technical users.

This shift has had a significant impact for people and communities around the world. For instance, people who cannot code can now instruct computers to perform complex tasks, and people who are blind or have low vision can receive descriptive output that describes the content of pictures or text.

For human rights, the implications of multi-modal AI are immediate. A sample of the rights-supporting benefits are listed below.

Disability rights: AI-powered assistive technologies including real-time captioning, speech-to-text, text-to-speech, navigation, communication aids, and cognitive support can uphold the CRPD rights that current systems fail to deliver. The trade-off is that always-on assistive AI requires significant personal data. However, this risk should be managed through design rather than used as a reason to withhold the technology.

Access Quest — disability data collection done well¹⁷⁷

Access Quest is a disability-led data collection project developed in Aotearoa New Zealand to map the accessibility of the built environment from the lived experience of disabled people. The data is gathered by disabled contributors, governed by the disability community, and used both for advocacy and for the practical purpose of routing around inaccessible places. The case demonstrates that the participation principle in PANEL is not just a procedural thing. When the people most affected by a problem hold the data-collection design, the resulting dataset is more accurate, more useful, and less likely to embed the incorrect assumptions that disabled people routinely have to correct. The same principle applies to AI training data, evaluation benchmarks, and assistive technology design. The framework's recommendation is not to use AI on behalf of disabled people but to enable disabled people to govern the systems that affect them.

Digital literacy: The ability to interact with computers through natural language collapses some of the knowledge barriers between technical and non-technical users. A policy analyst can now interrogate a dataset in plain English, a community organisation can build a website, and a student can explore complex concepts through conversation.

Education: AI tutoring systems, adaptive learning platforms, and content generation tools can personalise education in ways that serve learners with different needs, paces, and languages. These systems must be designed with equity and cultural sensitivity in mind, and they must not replace human teaching relationships. However, there is significant potential for these tools to support ongoing and personalised education experiences for a wide range of learners.

Te reo Māori and Indigenous language technology

The intersection of AI and te reo Māori is a vivid illustration of the opportunity offered by AI and digital technology when developed by and for Māori. While minority languages are often excluded from or late to be added to digital products, community-owned or iwi-owned AI offers significant opportunities for bolstering and supporting the accessibility of te reo Māori in digital spaces, and fostering intergenerational language transmission.¹⁷⁸

Projects like Te Hiku Media's Papa Reo platform have garnered international attention as a world leader in Indigenous AI for their sophisticated natural language processing tools and cutting-edge data science grounded in mātauranga Māori and community-led processes. When developed and deployed with care and integrity, these projects can help realise numerous rights elaborated in the United Nations' Declaration on the Rights of Indigenous Peoples, and give effect to Te Tiriti o Waitangi.

Te Hiku Media and the Papa Reo platform¹⁷⁹

Te Hiku Media — born from the 1989 Waitangi Tribunal WAI 11 (te reo Māori claim) and the 1994 Privy Council broadcasting case — developed speech recognition for te reo Māori, achieving over 90% accuracy. Their platform Papa Reo enables indigenous language communities to “develop their own speech recognition and NLP capabilities, ensuring that the sovereignty of the data remains with them and the benefits derived from these technologies go directly to their communities”.¹⁸⁰ Big tech companies “have all failed to provide quality NLP tools for indigenous languages due to their failure to engage and grow the capability of the community”.¹⁸¹ Te Hiku Media succeeded because its project was indigenous-led and grounded in community values.

Kaituhi — the resulting transcription tool — is “the best model in the world for transcribing te reo Māori.”¹⁸² It empowers Māori research with interview transcription and supports whānau to preserve their history. The Kaitiakitanga License governs its use, prohibiting surveillance, tracking, discrimination, or building Māori corpora from the platform — “like open source but with affirmative action”.¹⁸³

Healthcare

AI in healthcare represents one of the clearest cases of technology directly serving the right to the highest attainable standard of health (ICESCR Art. 12). AI prescription safety tools can catch dangerous drug interactions that manual processes miss. Diagnostic AI can identify conditions from medical imaging with accuracy that supplements clinical judgement. Administrative AI can reduce the burden of paperwork that keeps clinicians from patient care.

However, AI in healthcare also presents risks that include: bias in training data that can reproduce health inequities, particularly for Māori; opacity of diagnostic systems; accountability when AI-assisted clinical decisions go wrong; privacy of health data used for model training. Development and deployment of AI tools in healthcare must be careful, tested, and consider the risks to people and communities.

Access to information and transparency of government

The right to seek, receive, and impart information (ICCPR Art. 19) is one of the rights most directly served by digital technologies. The Official Information Act 1982 and the Public Records Act 2005 cover digital and technology-based formats as part of their transparency requirements. Open data portals, platforms like FYI.org.nz for OIA requests, and digital court publishing systems all use technology to make government more transparent. While AI can reduce transparency in some contexts, it can also be a tool to enable transparency.

AI adds specific capabilities. Semantic search over large document collections can surface information that keyword search cannot. Translation and summarisation tools can make complex government documents accessible to non-specialist audiences. Automated monitoring can track regulatory compliance, government spending, or legislative change at a scale that manual monitoring cannot achieve.

Rules as Code and Better Rules — Aotearoa as a global originator

Better Rules, and the broader Rules as Code movement, originated in the New Zealand Service Innovation Lab in 2018¹⁸⁴. The idea is that the rules that govern a benefit, a licence, or a regulatory decision should be expressed in machine-readable form alongside the human-readable text, so that the same logic that drives a service to citizens drives the policy debate that shaped it. The approach has been picked up by Australia, the European Union, Singapore, Japan, Dubai, and French Polynesia. For human rights, Rules as Code has two faces. As an enabler, it aims to improve consistency, makes review more tractable, and exposes hidden discretion in administrative systems. As a risk, it can hard-code mistakes at scale and obscure the policy judgement underneath the code. The consequences can be equally significant, requiring equivalent safeguards.

Community empowerment and shifting power

When deployed effectively, AI and other digital technology can support the capacity of communities to address issues themselves — shifting power toward people and groups that may face marginalisation in the current system. This can include things like the ability to undertake community-driven research, access and interpret large data sets, and fix problems collectively rather than waiting for funding or government provision.

This kind of community empowerment and problem solving is already happening in specific contexts: Te Hiku Media is building language technology for te reo Māori. Community organisations are using machine learning for environmental monitoring, and building their own dashboards and websites without technical expertise. The conditions that best support these outcomes include community ownership of the project, Māori or community governance over data, technical capability within the community, and state support that enables rather than directs.

Centre of Machine Learning for Social Good¹⁸⁵

The University of Auckland's Centre of Machine Learning for Social Good, working with local councils, communities, and others, has built a portfolio of applied machine learning projects that do not look like the popular image of AI. The projects — including models predicting air-quality exceedances and freshwater quality thresholds, models supporting early intervention on school attendance, the Our Voices project documenting community concerns, and the taiao.net environmental-data infrastructure — demonstrate the breadth and depth of machine learning. The Centre's approach embodies a human rights-based approach, with participation, accountability, and non-discrimination as key values embedded across its work.

The benefits are concrete: cleaner air, faster response to environmental hazards, higher attendance of children in school, communities heard. The complexity is that this work depends on data infrastructure, ongoing funding, and institutional partnerships that are often invisible until they fail.

The rights foundation for promoting AI and other digital technologies

The State's duty to fulfil human rights (described further below) means that opportunities to promote and protect rights through AI and digital technologies are not optional extras. Where technology can materially advance the progressive realisation of economic, social, and cultural rights — in health, education, work, social support, environmental protection — and where the risks can be identified and managed, the State has an obligation to pursue those opportunities within its maximum available resources.¹⁸⁶ In addition, restrictions on digital technologies including bans, content filters, and mandatory access for law enforcement should be subjected to the same human rights limitation tests that apply to restrictions on any right.

This does not mean adopting every AI tool or deploying every automated system. It means ensuring that the governance architecture discussed in this report is designed not only to prevent harm but to enable benefit. A governance framework that is so cautious it prevents the deployment of rights-promoting technologies fails the people it is meant to serve.

Who is responsible for realising human rights in relation to AI and digital technology?

AI tools and other digital technologies should be designed, developed and deployed to be consistent with the obligations of states and the responsibilities of private actors under international human rights law.¹⁸⁷ In human rights law and practice, the term ‘duty bearer’ is used to denote who holds the responsibility for realising human rights. The term emerged from late 20th-century human rights law and practice, especially through the work of the United Nations, to describe those obligated to respect, protect, and fulfil human rights.¹⁸⁸ This contrasts with ‘rights holders’ — the individuals or social groups that have particular entitlements in relation to specific duty-bearers.

States are the primary duty bearers of human rights, including in relation to AI and digital technologies. Non-state actors (e.g. corporations, international organisations), also have responsibilities in certain contexts — this is especially important as most of the AI and digital technology this report addresses is built, sold, deployed, and operated by private companies.¹⁸⁹ Individuals can also have responsibilities in specific contexts. The responsibilities are asymmetric and shared, and they run across the whole lifecycle of AI and digital technology systems. Below, we outline the core obligations of states and other actors in relation to the development, deployment, and operation of AI and digital technology systems.

States’ core human rights obligations

The duty to respect, protect, and fulfil

The legal obligation and the primary responsibility to promote and protect human rights and fundamental freedoms lie with the State. States are the ones who ratify and are bound by human rights treaties and have obligations through their membership of the United Nations and other intergovernmental bodies.¹⁹⁰

States have three core obligations under international human rights law¹⁹¹ when it comes to individual human rights:

The Duty to Respect: This is a negative duty, requiring states to refrain from interfering with the enjoyment of rights. Governments must not take actions that directly violate specific rights. For example, states should refrain from arbitrary surveillance, censorship, or unjust restrictions on freedom of expression, as these undermine privacy and democratic participation.

Examples of how the duty to respect could be applied in relation to AI and digital technologies:

- Governments should avoid deploying AI-driven facial recognition in public spaces without strict necessity and proportionality tests.
- Governments should ensure algorithms used in social security decision making do not arbitrarily deny benefits without human oversight, respecting the right to social security.

- Governments should not interfere with the enjoyment of technology, such as arbitrary internet shutdowns or application blocking, except in limited situations. Any limitation should be necessary, evidence-based, and proportionate based on risks to safety, dignity, or freedoms of others, and should be no more restrictive than necessary to address that risk.¹⁹²

The Duty to Protect: This is a positive duty, requiring states to shield individuals from human rights abuses by third parties, such as corporations or private actors. States must enact laws, regulations, and enforcement mechanisms to prevent harm.

Examples of how the duty to protect could be applied in relation to AI and digital technologies:

- Governments should regulate AI companies to prevent discriminatory algorithms, misuse of personal data, or exploitative practices.
- Governments should require tech companies to conduct human rights impact assessments for AI systems used in recruitment, ensuring they do not discriminate based on gender or ethnicity.
- Governments should enforce transparency obligations for AI-driven credit scoring to prevent unfair denial of loans by banks protecting economic rights.

***Yorston v Attorney-General*¹⁹³: judicial review reaches inside the machine**

In *Yorston v Attorney-General*, the Court of Appeal confirmed that computer-generated Criminal History Records produced by the Ministry of Justice's case-management system are an exercise of executive power amenable to judicial review. The system is used daily by police, the courts, and judges in sentencing. The Court held that the Ministry has ultimate responsibility for the accuracy of the records the system produces. The decision matters because it forecloses an argument that has done a great deal of damage in other jurisdictions: that automation is "merely mechanical" and therefore lies outside the supervisory reach of public-law remedies. The Court of Appeal said the opposite — that the courts' constitutional responsibility to ensure officials act within their conferred powers applies more obviously, not less, where consistency and accuracy of administration are at stake.

The Duty to Fulfil: States must take proactive measures to facilitate and ensure the full enjoyment of human rights, including by creating enabling environments, facilitating access to necessary resources and services, and ensuring effective remedies for violations. For example, states should invest in digital literacy programmes, ensure equitable access to technology, and embed human rights standards in AI governance frameworks so everyone — including the most marginalised groups — can benefit from technological advancements.

Some human rights must be guaranteed immediately and in full, such as the right to life and freedom from torture or cruel, inhuman or degrading treatment. By contrast, economic, social and cultural rights, such as housing and health, are subject to progressive realisation, meaning not all aspects must be fulfilled at once. However, states are required to take deliberate, concrete and measurable steps towards full realisation, using the maximum of available resources.¹⁹⁴ Progressive realisation

does not justify inaction: each right has immediate core obligations which must be realised straight away. For example, primary education must be available and free to all immediately,¹⁹⁵ and states must immediately remove unjustified barriers to accessing scientific knowledge, its applications, and related goods, services and information.¹⁹⁶ In short, the framework allows flexibility in how and when rights are delivered, while holding states accountable for meeting essential minimum standards and making genuine progress.

This third duty is the one most often understated in AI policy. Where AI and digital technologies serve the realisation of rights, the State has an obligation to ensure conditions exist for people to benefit from them on terms that respect their rights, their agency, and their values. Examples run through health, education, expression, participation, accessibility, te reo Māori, and equal access to public services. The procurement, regulatory, and oversight levers of the State put both sets of duties into effect, so that the burden of vindicating rights does not fall on rights-holders.

Examples of how the duty to fulfil could be applied in relation to AI and digital technologies:

- The New Zealand Government could actively invest in domestic AI capability to nurture homegrown AI systems which uphold and promote human rights and Te Tiriti o Waitangi by design.
- The New Zealand Government could fund programmes to improve AI literacy among rural and Māori and Pacific communities, ensuring equitable access to technology and supporting digital inclusion.
- Governments should create clear complaint mechanisms for individuals harmed by algorithmic decisions, or empower already existing mechanisms to hear these types of complaints, fulfilling the right to an effective remedy. To some degree, Private entities also bear this obligation to some degree, as discussed below.

Meaningful and ongoing Māori involvement in the design, governance and oversight of digital infrastructure is an important expression of the Crown's obligations under Te Tiriti o Waitangi and its duties to respect, protect and fulfil human rights. This requires not only avoiding interference with Māori rights and interests, but also actively protecting them and creating the conditions for Māori to exercise rangatiratanga and benefit equitably from digital and AI innovation.

The private sector's human rights responsibilities

The specific duties of the private sector in relation to AI and digital technologies are outlined in part in the UN Human Rights Council's 2025 'new and emerging digital technologies' resolution, which reiterates that businesses must avoid causing or contributing to adverse impacts and seek to prevent and mitigate impacts linked to their operations, products, and services via business relationships.¹⁹⁷ It calls on digital technology companies and developers to apply human rights due diligence (HRDD) across the technology life cycle. UN reporting emphasises that businesses cannot "outsource" these responsibilities merely by using a third-party AI system.¹⁹⁸ It is important to emphasise here that unlike some other fields, some technology companies now wield state-like economic power¹⁹⁹ and the growing concentration of digital markets means technology companies have unprecedented power over trade, communication, information, and innovation.²⁰⁰

UN AI governance literature also broadens who counts as an accountable actor by adopting a lifecycle or value-chain lens. UNESCO defines ‘AI actors’ as anyone, natural or legal persons, participating in any stage of the AI lifecycle (from research and design through deployment, monitoring and evaluation, trade and financing).²⁰¹ Complementing this, a UN Working Group report focuses on AI procurement and deployment, clarifying that both states and businesses that procure or deploy AI — even if they do not develop it — must apply the UN Guiding Principles on Business and Human Rights framework.²⁰²

Principles and frameworks for understanding the human rights responsibilities of the private sector

The UN Guiding Principles on Business and Human Rights (UNGPs),²⁰³ endorsed by the UN Human Rights Council in 2011, is the leading framework internationally for digital-technology harms. It provides a globally recognised normative framework which sets out human rights responsibilities of the private sector. The UNGPs lay out a set of principles for businesses to prevent, mitigate, and remediate human rights risks, including those arising from the development and use of AI.²⁰⁴ The principles apply to all businesses across sectors and geographies, offering a principled yet flexible framework that can be adapted in the context of developing, deploying, and using new technologies.²⁰⁵

The OECD Guidelines for Multinational Enterprises (2023 revision),²⁰⁶ the OECD Due Diligence Guidance for Responsible AI (2025),²⁰⁷ and the European Union triad of the AI Act²⁰⁸, the Corporate Sustainability Due Diligence Directive²⁰⁹, and the Digital Services Act²¹⁰ all put the UNGPs into binding effect for the businesses operating inside them. Aotearoa New Zealand businesses operating internationally are already subject to that regime, and compliance with such regimes is an essential part of becoming a global company.

The HRDD process is the key mechanism by which businesses fulfil their responsibility to respect human rights. It is a continuous, proactive process involving four core steps — human rights risk identification and prioritisation, integration and action, tracking effectiveness, and communication. In the context of AI, this means assessing risks before system design and throughout the lifecycle. Without proper due diligence, AI systems can exacerbate bias, discrimination, and opacity in decision-making. The complexity and rapid evolution of technology and AI models make it hard to foresee all potential harms. This necessitates an anticipatory, iterative due diligence process tailored to both the technology and its societal context.²¹¹

Collective and individual rights holders

Aotearoa New Zealand’s human rights framework is both individual and collective. Common Article 1 of two international covenants — the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights — opens with the collective right of peoples to self-determination. Article 29 of the Universal Declaration of Human Rights places duties to the

community at the heart of the framework. The UNDRIP²¹² makes the joint individual-and-collective character explicit. In relation to specific duty-bearers, the individuals and collective groups who have particular entitlements are known as ‘rights holders’. While all human beings are rights holders under the Universal Declaration of Human Rights, there are also often specific groups of rights-holders whose human rights are not fully respected or realised.²¹³

The collective dimension is decisive in practice for AI. AI derives its reach from patterns identified across populations, not from the individual data points it collects, and one person’s data routinely implicates others. Whakapapa is the strongest articulation of this point. Te Mana Raraunga’s Māori Data Sovereignty Principles (2018)²¹⁴ and Te Kāhui Raraunga’s Māori AI Governance Framework (2025)²¹⁵ state the working rule for Aotearoa New Zealand: individuals’ rights are balanced with those of the collectives to which they belong, and in some contexts collective Māori rights will prevail. This is the case under any human rights framework, and any human community living together.

Whole-of-society action to balance the opportunities and risks

The framework presented by human rights and Te Tiriti o Waitangi holds risks and opportunities together. AI and digital systems impose real risks on rights, including risks at scale. They also create real opportunities to advance rights, including for people whose rights have historically been undermined. This report addresses both the risks and the opportunities — identifying what must be protected, what should be promoted, and what structural changes are needed to make both possible.

Where AI and digital systems can deliver health, education, justice, and information services that would otherwise be unavailable or of poorer quality, the duty to fulfil is engaged on the opportunity side — the opportunities should not be considered only as a counterpoint to the risks. A governance response that prevents beneficial uses without proportionate justification is itself a failure to fulfil rights obligations.

The proportionality test, which balances the right impaired and the benefit secured, is what holds risks and opportunities together. The same test that asks whether a limitation on a right is justified also asks whether the absence of a permission is justified. The commission’s view is that the test must be applied symmetrically, with risks and opportunities held in balance and no one human right elevated over another.

Aviation safety as a model for AI risk governance — dedicated illustration

Aviation is a useful illustration of how a society chooses to make a high-risk technology routinely available. The risks are real: a Boeing 737-800 crash that killed all aboard would be, in any other sector, a national emergency. But society has chosen to fly, and what has made that choice sustainable is the safety and regulatory framework built around it.

The aviation safety regime has four features that translate directly to AI governance:

Mandatory incident reporting requires operators and other aviation participants to disclose safety events to a national authority, the Civil Aviation Authority (Civil Aviation Act 2023, s 49; Civil Aviation Rules Part 12).²¹⁶

A no-blame reporting policy protects individuals who report in good faith — their notifications can't be used as evidence against them in criminal proceedings, and the regulator may only pursue enforcement where the public interest in doing so outweighs the chilling effect on future reporting, subject to exceptions for reckless or repeated misconduct (Civil Aviation Act 2023, s 12(9)(h), ss 339–341).²¹⁷ This encourages the surfacing of near-misses rather than their concealment, though it protects the reporting individual rather than granting the operator blanket immunity.

Independent investigation — through the Transport Accident Investigation Commission (TAIC), a body established under its own 1990 Act — separates safety inquiry from regulatory enforcement and from the operators concerned. The Civil Aviation Authority must notify the TAIC of every accident or incident, and its own investigative powers give way to the TAIC's (Civil Aviation Act 2023, s 23(e), s 50).²¹⁸

Cross-sector learning means that what one operator learns about a failure mode is shared across the sector through airworthiness directives and director-mandated training updates issued after a safety review, so the fix reaches every operator, not just the one that discovered the problem (Civil Aviation Rules Part 39; Part 61, Subpart I).²¹⁹

The result is a system in which the safety of the whole sector improves through use, rather than degrading through use. The Civil Aviation Act 2023 supplies much of the statutory basis for these no-blame reporting protections, with the Transport Accident Investigation Commission Act 1990 supplying the remainder.²²⁰ Together, they give operators a real incentive to report rather than conceal, without collapsing the system's ability to hold genuinely reckless conduct to account.

For AI, the same design is available. A national approach to AI harm reporting — operators submit notifications of consequential failures, the information is held by an independent body, the body publishing anonymised lessons across the sector, and reporting that attracts statutory protection from secondary liability — would build the same compounding-safety dynamic the aviation sector has built over decades.

The case also illustrates that high-risk does not mean unavailable. Aviation safety is the reason flight is routine. AI safety could be the reason AI use is routine, on terms the country is willing to live with.

Something else that can be learned from the aviation sector is how to guard against skill decay and over-reliance on automation. Pilots must periodically demonstrate they can still fly and make decisions without relying solely on their aircraft's automated systems — through recurrent competency checks, currency requirements, and biennial flight reviews, on top of the initial licensing tests (Civil Aviation Rules Part 61, rules 61.37, 61.39). 221 A similar principle could apply to operators of AI systems: periodic, independent verification that a human operator retains the skill and judgement to intervene, rather than assuming initial training or certification is sufficient for the life of the system.

How this approach informs our recommendations

The critical opportunity being pursued through this report is to move the discussion on digital technology toward a conversation about AI and technology that leads to actionable change and embeds the broad human rights-based approach principles of participation, accountability and transparency, non-discrimination and equality, empowerment, and legality. This conversation requires meaningful engagement, not only between government and experts, but with the communities whose lives are shaped by these technologies. Meaningful engagement, in turn, requires meaningful information — transparency about what systems exist, education that builds genuine comprehension, and the practical conditions for people to make informed choices about how they interact with technology and how it interacts with them. This has informed our approach to the recommendations that follow.

Actions to bring effect to a rights-based approach to AI and digital technologies

In this section, the commission makes two key recommendations and outlines three system enablers for implementing a rights-based approach to planning, developing and implementing AI and other digital technologies in Aotearoa New Zealand. For the system enabler, the commission suggests a range of actions which complement, and sit alongside, the key recommendations.

The recommendations and system enabling actions are aimed at the Government, which is both the duty bearer and holder of many of the levers required to progress work in these areas. However, it is important to note that a whole-of-society approach is required: everyone has a role to play. We expect that public sector organisations, businesses, non-governmental organisations, iwi and hapū, communities and individuals will all see areas in these actions where they can make an active contribution. The recommendations are deliberately calibrated to anticipate an ongoing and constructive role for all of these groups.

The recommendations and system enabling actions below represent the position of the commission. They were developed with significant input from the Expert Advisory Group and wider engagement with a range of domestic and international experts (See **Appendix One** for full list).

There has already been significant work done in Aotearoa New Zealand to build the foundations for technology systems that align with a rights-based approach to AI and other digital technologies. The work in front of Aotearoa New Zealand is the work of implementation — using the existing framework, applying it consistently across the choices these technologies require, resourcing the institutions that operate it and filling gaps where needed.

Overview of recommendations and priority areas for action

The commission makes the following recommendations:

- **Recommendation One:** Develop a national digital infrastructure strategy anchored in human rights and Te Tiriti o Waitangi.
- **Recommendation Two:** Develop a national approach to risk assessment and mitigation for AI and digital technologies, anchored in human rights and Te Tiriti o Waitangi.

The commission considers the following three system enablers as foundational:

- Empower people and communities to shape how AI affects their lives.
- Strengthen government leadership and accountability.
- Address legislative and regulatory gaps.

Figure 1 summarises the structure of the recommendations and how they work together to advance AI and digital technologies that are consistent with Te Tiriti o Waitangi and human rights in Aotearoa New Zealand. It shows how priority recommendations are supported by key system enablers and grounded in human rights and Te Tiriti. Further information about each of the recommendations and system enablers is provided below.

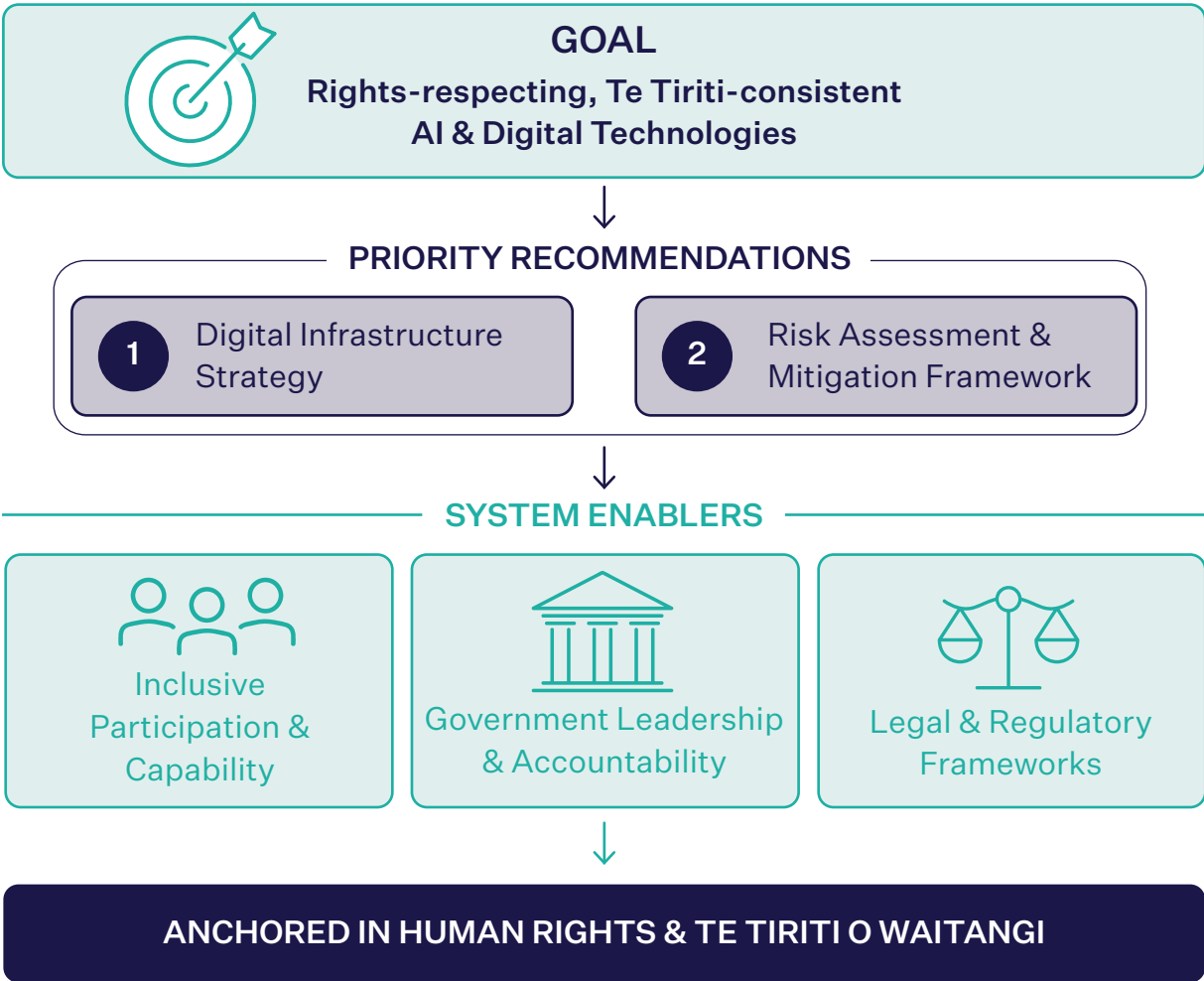


Figure 1 Overview of recommendations

Recommendations

Recommendation One: Develop a national digital infrastructure strategy anchored in human rights and Te Tiriti o Waitangi

Key actions

1. Develop a whole-of-society national digital infrastructure strategy with explicit human rights and Te Tiriti foundations that upholds Māori data sovereignty, has a long-term planning horizon in line with Aotearoa New Zealand's other infrastructure planning, and enables our digital sovereignty.
2. Establish one point of accountability to advance and coordinate the development of the strategy.

Background and analysis

Digital infrastructure is a global system that includes hardware, software, connectivity, computer, and data centres, along with common protocols by which information systems connect.

At the moment, the digital infrastructure that Aotearoa New Zealand relies on was developed piecemeal through the accumulation of individual local and international business and procurement decisions, and unrelated departmental programmes. Aotearoa New Zealand does not plan for and build other infrastructure like roads, water, electricity networks, the courts or the school system on an ad hoc basis. It should not approach digital infrastructure that way either.

A national digital infrastructure strategy would mean that a strategic approach could be taken to guide investment in domestic capability, enabling active and enduring participation in the development and delivery of local solutions rather than defaulting to being a consumer of AI systems designed elsewhere for other contexts. This may include developing aspects of local ownership or governance of the AI system, in line with approaches known as 'sovereign AI', 'Public AI', or 'AI agency'.

Sovereign AI, Public AI, and AI agency

The term 'sovereign AI' is used in several overlapping ways, but it is popularly understood as a country or organisation's capacity to develop, deploy and govern AI using its own infrastructure, data and people, and to reduce its dependence on systems controlled from offshore.²²² Understood more fully, it is less about any single asset or AI model than about autonomy and control across a number of dimensions: where systems are hosted and under whose jurisdiction; whether access can be revoked or interrupted by others; the cost and equity of access; privacy and information security; the strength of governance and independent oversight; whether a system's design and training reflect local and indigenous values; how far it can be customised to local needs; and the environmental and supply-chain dependencies that sit behind it. Understood this way, 'sovereignty' is less about a claim that a country should build everything itself but rather a label for a set of questions about agency, self-determination and control.²²³

These questions carry human rights and Te Tiriti implications as well as technical or economic ones. Who controls an AI system influences whose values are

embedded in it, whose data it is trained on, and how rights such as privacy, freedom of expression and freedom from discrimination are protected or placed at risk. It also shapes who is accountable when a system is wrong, biased or harmful. For Māori, these concerns connect directly to Te Tiriti o Waitangi and to Māori data sovereignty, and to the guarantee of tino rangatiratanga over taonga, including te reo Māori and mātauranga Māori. Decisions about hosting, training data, content moderation and access are, in this sense, also decisions about rights and about the Crown–Māori relationship.

Initiatives to develop or build sovereign AI systems have been uneven internationally. The United Kingdom and Canada have each committed on the order of £2 billion and CAD\$2 billion to sovereign AI, though much of that has funded public compute while day-to-day governance remains with private, often foreign, providers — Canada’s Cohere data centre, for example, is operated by the United States firm CoreWeave. A different approach is represented by fully open, publicly governed systems such as Switzerland’s Apertus and the Allen Institute for AI’s OLMo, which release their model weights, training data and code openly. In Aotearoa New Zealand, one commonly cited example is Te Hiku Media, whose Papa Reo language platform and Kaituhi transcription tools run on dedicated, onshore infrastructure, over data the organisation itself controls, under governance arrangements — notably the Kaitiakitanga Licence²²⁴ — designed so that the benefits of the technology return to the people and the kaupapa that produced it. It is often described as an operational example of indigenous data and AI sovereignty in practice.

There is also a live debate about whether ‘sovereignty’ is even the right frame. Australia’s Tech Policy Design Institute (TPDi), in *From AI Sovereignty to AI Agency* (2025),²²⁵ argues that ‘sovereignty’ tends to be treated as binary — a country either has it or does not — which leaves most nations looking disempowered, and that the term is used too inconsistently to guide policy. TPDi proposes reframing the goal as ‘AI agency’, defined as a country’s capacity to shape its AI future and steer outcomes within a globally connected system. In the ‘AI agency’ model, power comes from the ability to shape relationships rather than from self-sufficiency, and the aim is not to lead in every capability but to understand a country’s genuine strengths, reduce critical dependencies, and build leverage where advantages exist.

The Public AI Network offers a third potential reframing in its white paper *Public AI: Infrastructure for the Common Good* (2024),²²⁶ which argues that societies can create the AI technologies that shape their lives rather than only consuming those built by a handful of unaccountable firms. The Public AI Network argues that AI should be treated as public infrastructure in the tradition of railways, electricity and public broadcasting. It defines ‘public AI’ by three essential features: public access (affordable, near-universal access to capabilities essential for participation in public life), public accountability (ultimate control of development resting with the public), and permanent public goods (funded and operated so that what they produce endures). This understanding of AI as public infrastructure shares some similarities with the commission’s approach and recommendations.

A multistakeholder-developed national digital infrastructure strategy, anchored in human rights and Te Tiriti o Waitangi, would provide a mechanism to articulate Aotearoa New Zealand's vision for digital infrastructure and allow for long-term coordination. It would also enable Aotearoa New Zealand to better navigate both the opportunities and the risks of AI and digital technologies in an ever-changing landscape of technology developments, now and into the future. In the proposed national digital infrastructure strategy, we suggest an approach where Aotearoa New Zealand owns the vision, design and development, regulatory framework, and monitoring of its implementation. This approach is also in line with Aotearoa New Zealand's obligations under the ICESCR, including the right to enjoy the benefits of scientific progress and its applications.²²⁷

A national digital infrastructure strategy would allow the international complexity of the system and all its components to be considered collectively at a domestic level. It can include consideration of the technical standards for interoperability that allow the components to work together, the governance frameworks that determine how human rights and Tiriti obligations are honoured in their operation, the trust frameworks that allow people to participate in them, and the regulatory architecture for the systems running on the infrastructure. The scope of the strategy should include all digital infrastructure, with AI being just one layer within this overall system.

The EuroStack initiative and the geopolitics of digital sovereignty

The EuroStack initiative is an example of an all-of-EU effort to assemble a stack of digital infrastructure — cloud services, identity, payment, AI capability — that is not contingent on the goodwill of any single foreign jurisdiction. GAIA-X, the European federated cloud project, sits inside that effort. The motivation is in part economic and in part defensive: the United States CLOUD Act, the European Court of Justice's Schrems decisions on data transfer,²²⁸ and the increasing strategic use of digital infrastructure in trade and security disputes have made the limits of borrowed sovereignty visible.

This demonstrates that other jurisdictions are increasingly considering how digital systems should be understood and governed as critical infrastructure, rather than simply as a collection of private technologies or commercial services.

In suggesting that AI and other digital technologies be treated as public infrastructure, we are mindful that historically, Māori have been adversely impacted by alienation of land and other actions in the name of the public good.²²⁹ This further underscores the importance of a Tiriti-based approach to governance of digital technologies as public infrastructure, which ensures Māori have a voice in the governance arrangements and decision-making processes.

The commission considers that the Government should appoint a responsible Minister, agency or Crown Entity to coordinate and advance this work. The current restructuring of digital areas of responsibility in government is an excellent opportunity to advance a whole-of-society approach. The strategy itself must be developed through a multi-stakeholder process in line with the human rights-based approach (HBRA) to be effective.

The commission notes there is ample work within and beyond government which could be brought together in the strategy process, including: Te Mana Raraunga's Māori Data Sovereignty Principles (2018),²³⁰ Te Kāhui Raraunga's Māori Data Governance Model (2023)²³¹ and AI Governance Framework 2025²³² (including its "IT infrastructure that works for Māori" pou), Te Hiku Media's Papa Reo and Kaituhi infrastructure,²³³ and the wider iwi-led data governance work.²³⁴ The AI Forum's *AI Blueprint for Aotearoa: A Refreshed Vision to 2030* (May 2026)²³⁵ is a substantial industry articulation that would contribute to the work recommended. The Government Digital Target State,²³⁶ and the establishment of the Government Digital Delivery Agency (GDDA) on 1 April 2026 is a significant reorganisation contributing to the modernisation of the government's own digital architecture.

The Human Rights Act²³⁷ requires the commission to undertake a national human rights action plan (NHRAP) for the promotion and protection of human rights in Aotearoa New Zealand. We expect the next iteration of this plan will include digital technologies and AI in its scope, reflecting their significant transformational impacts on society. The NHRAP must be developed in consultation with interested parties including communities and the Government. This consultation process, already legislated for, could also act as a key way to engage with the public on the national digital infrastructure strategy and ensure that it supports human rights and Te Tiriti. The commission's independent status, clear human rights promotion mandate and Te Tūhonotanga agreement with the National Iwi Chairs Forum and relationships with key stakeholders, position it well to play a lead role in this work.

The key requirements of a NHRAP are that it covers the full geographic territory (so considers the rights of all people across Aotearoa New Zealand), that it upholds international human rights frameworks, that it is a forward-looking plan and that it provides tangible actions for stakeholders to carry out towards rights realisation. All of these aims would also align well with the needs of a digital infrastructure strategy. Given this the commission should be adequately resourced to undertake this work.

Scope of the digital infrastructure strategy

The exact scope of the strategy-setting process is beyond the scope of this report, but the commission recommends the following minimum requirements:

- 1. Leadership:** there must be a point of accountability for setting the strategy against a coherent human rights foundation. The strategy must be developed in partnership with iwi and hapū as collective rights-holders. Te Kāhui Raraunga and Te Mana Raraunga provide a starting point for that engagement, and should be engaged as co-designers, with the Māori Data Governance Model as a baseline requirement for any digital infrastructure that engages Māori data. A multi-stakeholder process should not mean diffusion of accountability. Leadership could be assigned within the public service, or at Ministerial level, but must include a multi-stakeholder approach extending beyond government and the public service to include the private sector, civil society, technical and research expertise, and communities. Leadership and decision-making for the strategy and the strategy-setting process should reflect Te Tiriti o Waitangi.
- 2. Participants:** government is a critical participant, but any strategy will lack legitimacy and be less likely to succeed if it fails to include people and communities from across society, in line with the HBRA's participation principle.
- 3. Collaborative process:** the strategy-setting process must be legitimate and support meaningful and equitable participation. The commission's process to develop a NHRAP for the promotion and protection of human rights in Aotearoa New Zealand could form the basis of meaningful community engagement, if adequately resourced.
- 4. Analysis and research:** the strategy-setting process must be adequately informed by existing initiatives and frameworks, and should ensure all participants come to the process based on adequate information so their participation is meaningful.
- 5. Topics and scope:** the strategy must extend beyond AI and physical hardware to include the full digital stack as outlined above, and create space to grapple with and lay a foundation for coherent positions on the issues raised in this report, including:
 - a. a consistent approach to recognising and giving effect to Indigenous rights and Māori data sovereignty,
 - b. sovereign AI, Public AI, or AI agency capability,
 - c. the environmental impacts of large-scale AI infrastructure,
 - d. the foreign policy and international trade dimension to AI and digital technologies and the transnational nature of digital technologies and data hosting across jurisdictions, including their implications for national security and defence,²³⁸ and
 - e. the energy implications of AI and digital technologies.
- 6. Time horizon:** the strategy must be oriented toward a period of decades, not years, to sit above political, industry and technology cycles. This aligns with the time horizon Te Waihanga, the New Zealand Infrastructure Commission uses in its planning.

Key participants to deliver the recommendation

Cabinet; the Public Service Commission and the GDDA; the Treasury; Te Puni Kōkiri; Te Kāhui Raraunga and Te Mana Raraunga; iwi-led organisations; the Ministry of Foreign Affairs and Trade; the Ministry for the Environment; the Ministry of Business, Innovation and Employment; the Department of Internal Affairs; Te Waihanga; the Reserve Bank of New Zealand; Te Kāhui Tika Tangata Human Rights Commission itself.

Recommendation Two: Develop a national approach to risk assessment and mitigation for AI and digital technologies, anchored in human rights and Te Tiriti o Waitangi

Key action

- Adapt existing Aotearoa New Zealand frameworks and draw on international best practice in developing the national approach to human rights and Te Tiriti risk assessment and mitigation.
- Include both public and private sector entities in its scope.
- Adequately resource the commission, as Aotearoa New Zealand's independent national human rights institution, to play a leadership role in the development of a national human rights and Te Tiriti-based risk assessment for AI and digital technologies.
- Ensure this work is done in partnership with Māori and their representative organisations as Te Tiriti-rights holders, and with other relevant independent crown agencies.

Background and analysis

In addition to action at a government level, there are actions that can be taken by individuals, industry, agencies, and deployers of AI and digital systems. Risk and impact assessment²³⁹ is the key method recognised for putting human rights and Tiriti obligations to work in the design, development, deployment, and governance of AI and digital technologies.²⁴⁰

International best-practice for human rights risk assessments in this area systematically identify and assess impacts on human rights across the technology lifecycle, prioritising the most severe risks to people and incorporating meaningful engagement with affected rights-holders and stakeholders.²⁴¹ They typically contain: a description of the technology and its use cases; identification of affected rights and groups; assessment of likelihood, severity and scale of harm; stakeholder/rightsholder input; mitigation and governance measures; residual risks; monitoring and review mechanisms; and clear accountability and remedy pathways.²⁴²

Risk assessment is non-partisan, technically feasible, and grounded in a substantial body of practice in Aotearoa New Zealand and more widely in the international space. It is what gives the framework practical force at the level of an individual AI or digital technology deployment, procurement or programme. Risk and impact assessment tools provide a clear process for making key decisions in a consistent, rights-protecting way which mitigate harms. They also act as a key form of due diligence in making decisions whether or not to use a certain digital tool.

While there is already a wide range of risk assessment tools in place in Aotearoa New Zealand, the commission considers a coordinated national approach is required that could be used by any organisation deploying AI and other digital systems. This approach should be anchored in human rights and Te Tiriti and draw on the existing body of Aotearoa New Zealand guidance and standards. It should be developed in partnership with iwi-led organisations, communities, industry and the public service.

The commission considers that it is well-placed to help bring together a national risk assessment framework, if appropriately resourced to do so. This is in line with emerging international best practice as National Human Rights Institutions (NHRIs) are increasingly developing and promoting human rights impact assessment approaches for AI and digital technologies in line with their mandates to protect and promote human rights.²⁴³ Notably, the National Human Rights Commission of Korea has issued Human Rights Guidelines on the development and use of AI and subsequently developed a comprehensive human rights impact assessment tool for AI.²⁴⁴ Similarly, the Danish Institute for Human Rights has produced detailed guidance on conducting Fundamental Rights Impact Assessments for high-risk AI systems,²⁴⁵ while the Equality and Human Rights Commission (Great Britain) has developed guidance for assessing the equality impacts of AI-based technologies in public services, among other examples.²⁴⁶

Three operational scoping questions remain open and require engagement to settle: the scope of rights covered by the assessment duty, the risk-level thresholds that trigger different assessment tiers, and the technologies in scope. The commission considers that these can be appropriately settled through broader participatory engagement, recognising a particular role for iwi and hapū as Tiriti partners.

Given the State is the primary duty-bearer in human rights terms, the outcomes of the human rights assessments must be binding on the public sector. In the short term, risk assessment mechanisms will not lead to binding legal consequences in the private sector unless legislation is passed in order to action this. However, accountability mechanisms can be added in stages as the risk assessment framework matures. These mechanisms could include transparency duties, independent audit, public registers, harm reporting, statutory force for the assessment duty, and redress for harm caused.

Risk assessment tools that can be drawn on when developing a national approach

The risk assessment tools already in place in Aotearoa New Zealand include:

- The Algorithm Impact Assessment toolkit and Algorithm Threshold Assessment developed by Stats NZ,²⁴⁷
- The Ministry of Social Development's *Privacy, Human Rights, and Ethics* framework and *Automated Decision-Making Standard* (this is the most developed agency-specific impact-assessment regime in the country),²⁴⁸
- The Privacy Commissioner's *Biometric Processing Privacy Code 2025*, which imposes a binding proportionality assessment,²⁴⁹
- Responsible AI Guidance for the Public Service: GenAI,²⁵⁰
- The Aotearoa New Zealand GenAI Research Guideline,²⁵¹
- MBIE's *Responsible AI Guidance for Businesses*,²⁵²
- The Digital Identity Services Trust Framework,²⁵³ and
- Te Kāhui Raraunga's *Māori AI Governance Framework 2025*.²⁵⁴

Further detail about a sample of these frameworks is outlined below. Internationally, human rights risk assessments have a long history of use as part of human rights due diligence²⁵⁵ and are a central requirement of the UN Guiding Principles on Business and Human Rights.²⁵⁶ In relation to use within AI and emerging digital technologies, the following tools all build the same methodology into binding form in different way:

- the European Union’s Artificial Intelligence Act’s Fundamental Rights Impact Assessment,²⁵⁷
- the OECD’s *Due Diligence Guidance for Responsible AI* (2025)²⁵⁸,
- the Council of Europe’s Framework Convention on AI (CETS 225),²⁵⁹
- the Canadian Algorithmic Impact Assessment,²⁶⁰
- South Korea’s Human Rights Impact Assessment Tool for AI, introduced by the National Human Rights Commission of Korea,²⁶¹ (as discussed above) and
- All New South Wales (NSW) Government agencies must complete the NSW AI Assessment Framework, and high- or critical-risk AI systems must be reviewed by the NSW AI Review Committee.²⁶²

Te Kāhui Raraunga Māori AI Governance Framework

This framework outlines how Māori data sovereignty must extend to AI systems, in alignment with the following principles:²⁶³

- free, prior and informed consent (FPIC) for all Māori data use,
- recognition of collective privacy rights beyond individual privacy protections,
- Māori authority over data regardless of storage location or AI processing jurisdiction, and
- prohibition of generative AI tools built on Māori data without Māori involvement.

MSD Automated Decision-Making Standard and PHRaE

The Ministry of Social Development’s Automated Decision-Making Standard,²⁶⁴ supported by the Privacy, Human Rights and Ethics (PHRaE) framework,²⁶⁵ is perhaps the most developed agency-specific impact assessment regime. It requires identified human decision-makers for automated decisions, structured impact assessment before deployment, mandatory human alternatives, preserved appeal pathways, and a prohibition on the automated review of automated decisions. The Automated Decision-Making Standard exists because MSD is the agency where the largest number of consequential decisions per capita are taken about people in vulnerable positions.²⁶⁶ This case demonstrates that a national approach to risk assessment and mitigation is not theoretical. The components exist in operation inside the New Zealand public service.

Privacy Commissioner’s Biometric Processing Privacy Code 2025²⁶⁷

The Biometric Processing Privacy Code 2025 is issued under the Privacy Commissioner’s binding code-making power in the Privacy Act 2020. The Code imposes a proportionality assessment as a precondition for the lawful operation of a biometric processing system, requires consideration of cultural impacts on Māori, and treats the assessment as evidence of compliance rather than a

procedural step. This case demonstrates that binding rights-based assessment is operating in New Zealand law now, under an existing statutory mechanism. The Code is the proof of concept for Recommendation 2 in two ways: it shows that a national human rights risk assessment framework can be designed and implemented inside existing constitutional and statutory architecture, and it shows that the code-making model under s21 of the Privacy Act can be replicated for other consequential domains — including a Māori information and data privacy code.

Digital Identity Services Trust Framework²⁶⁸

The Digital Identity Services Trust Framework, established under the Digital Identity Services Trust Framework Act 2023²⁶⁹, is the strongest existing New Zealand model for binding assessment as a precondition of operation. A digital identity service may not present itself as accredited under the Trust Framework unless it has passed assessment against the Trust Framework rules — including rules on privacy, security, accessibility, and Tiriti partnership. The accreditation is optional but commercially valuable, which means the assessment is taken seriously in a way procedural-compliance frameworks often are not. The Trust Framework's decentralised design — multiple identity providers, each independently accredited, with consumers choosing between them — is itself a rights-respecting design choice, avoiding the centralisation of identity infrastructure that other jurisdictions have moved toward.

Key participants to deliver the recommendation

Te Kāhui Tika Tangata Human Rights Commission; the Government Chief Digital Officer and the GDDA; the Privacy Commissioner; Stats NZ; Te Kāhui Raraunga and Te Mana Raraunga; iwi-led organisations; the existing regulator network; the Crown Law Office; the Office of the Ombudsman; the academy; the public-service AI body; private-sector partners.

System enablers to support a rights-based approach to AI and digital technology

If put in place, the two key recommendations outlined above will make a significant contribution to ensuring that Aotearoa New Zealand deploys AI and other digital technologies in a coordinated, planned, rights-protecting way. However, they also rely on supporting actions in a range of cross-cutting system enablers that help create the conditions for success.

The three system enablers outlined below include a range of suggested actions that help mitigate the human rights risks outlined in this report and ensure people and communities are able to access the opportunities offered by AI and digital technologies. Together, they provide practical mechanisms and essential foundations for embedding human rights and Te Tiriti o Waitangi across the design, deployment, and governance of AI and digital technologies.

System Enabler One: Empower people and communities to shape how AI affects their lives

The framework requires that people whose rights it protects are empowered to put those rights into action. Empowerment is the foundation for every other recommendation and suggested action in this report. This priority area is about ensuring people and communities understand AI and human rights systems and have meaningful access to digital technologies. It also is about ensuring that coming workforce transitions are managed equitably and that the local technology sector has what it needs to design and deliver rights-respecting solutions.

The current societal transformations being accelerated by AI and digital technologies come at a time when there is already a significant digital divide. Without action to ensure people are digitally included, there is a risk this gap will widen further.

Building the foundations for empowered people and communities

AI and human rights literacy

The European Union's Artificial Intelligence Act (AI Act)²⁷⁰ defines AI literacy as follows: “‘AI literacy’ means skills, knowledge and understanding that allow providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause”.²⁷¹

Without the capability to understand a system, the knowledge to recognise that rights are engaged and the standing to act on that recognition, transparency is meaningless, consent is procedural, and the right to challenge an automated decision is hollow. The commission considers that AI literacy and human rights literacy are not separable from each other. People need to understand what these systems are, where they appear in their lives, and what they can do with their information.

The international obligation to promote AI literacy and understanding of human rights already exists. UNESCO's Recommendation on the Ethics of Artificial Intelligence²⁷² (Article 101) directs Member States to provide AI literacy education at all levels in order to empower people and reduce digital divides. It is important to note that promoting AI literacy and a drive to promote responsible adoption is not the same as compelling people to use AI in circumstances where they object or feel uncomfortable. AI literacy creates an opportunity for informed choice, including the choice not to use a certain tool or technological system.

Regionally, Singapore's approach to AI literacy in schools is to embed age-appropriate AI education across the curriculum and the national Student Learning Space, enabling students to learn about AI, learn to use AI, learn with AI, and learn beyond AI while emphasising critical thinking, ethics, safety, and responsible use.²⁷³

Meaningful digital access

Where AI and digital systems serve the realisation of rights (the right to information, to participate in cultural life, to share in the benefits of scientific progress, to access services and government), excluding people from those systems excludes them from the rights themselves. As more and more services are offered through digital channels, and as digital and AI tools open up opportunities to users, it is increasingly important that people have meaningful access to digital technologies and the internet, along with the capability to use them. Restricting access, whether by cost, geography, capability, or design, engages the human rights framework directly.

The Digital Equity Coalition Aotearoa New Zealand (DECA) records that at least one in ten people in Aotearoa New Zealand are digitally excluded²⁷⁴ and over one in five struggle to access necessary services to get on with life, with the harm concentrated on families on low incomes, seniors, Māori, Pacific peoples, disabled people, those new to Aotearoa New Zealand, and remote communities.²⁷⁵ The Department of Internal Affairs in its 2022 long-term insights briefing²⁷⁶ put the proposal that follows from this evidence on the record: digital access could be treated as a statutory human right, on the model of the Privacy Act 2020.

Meaningful choices and alternatives

Once someone has digital access and meaningfully understands the way that digital systems implicate their rights and interests, what choices are available to them? The right to make meaningful choices about which technological systems to participate in presupposes that there are alternatives, that the alternatives respect rights, and that movement between systems is possible.

If the only available system is one that does not respect rights, the choice to participate or not is not a meaningful one. The right to participate in technological change presupposes the right to decline particular technologies on principled grounds. The commission considers that the choice not to use AI must be protected, particularly in the delivery of essential public services and in contexts where non-use should not lead to disadvantage. This right is not necessarily absolute — all rights can be subject to reasonable limitations, but any limitation must be imposed following a human rights-based approach, for a legitimate

purpose, in a proportionate way, and subject to safeguards and protections.

The commission considers that interoperability, data portability, accessibility, and protected non-digital alternatives in essential public services are the structural foundation for any choice to be real. International commentary²⁷⁷ and the New Zealand Government itself²⁷⁸ recognise that government procurement is a powerful lever for driving change.

Practical Steps

Support iwi and hapū to exercise their self-determination, particularly in relation to Māori data sovereignty

This includes strengthening Māori capability, resources, and authority to govern Māori data and to influence the development and use of AI in ways that support the aspirations of iwi and hapū.

This may also include creating pathways for iwi and hapū to exercise authority over the collection, access, use, and governance of Māori data, and to meaningfully influence AI systems that affect their communities.

Advance digital inclusion

Require government agencies to identify and address digital exclusion, including through accessible design, affordability, capability-building, and targeted support for underserved communities.

Enable and resource community-led efforts to measure and monitor digital inclusion, and use this evidence to guide policy and investment.

Ensure AI, human rights and Te Tiriti o Waitangi literacy

Ensure people have the knowledge and capability to understand how AI and digital systems affect their rights, including their rights under Te Tiriti o Waitangi, by:

- identifying gaps,
- developing and delivering a plan to address those gaps, ensuring that the plan and the measures to address any gaps adopt a human rights-based approach.
- supporting and building of community-led and culturally adapted approaches to closing these gaps,²⁷⁹ and
- ensuring people have the skills and knowledge to understand, question, and make informed decisions about the AI and digital systems they encounter.

Encourage publication in machine-readable formats

Put in place support and accountability measures to make digital information available in machine-readable formats to support the use of digital systems, and to enhance accessibility for disabled people, in line with best practice²⁸⁰ by:

- encouraging the use of machine-readable formats so content works with assistive technologies and AI tools,
- making sure access to these formats is not unnecessarily restricted just to prevent AI scraping, and
- expanding access to digital information in ways that empower disabled people.

Support equitable workforce transitions

Research and assess how AI and automation might change jobs in key industries, with a focus on:²⁸¹

- identifying new economic opportunities and how New Zealanders can be supported to access them,
- understanding which industries have higher concentrations of particular groups (including Māori and Pacific Peoples) and recognising that job loss affects not just individuals but their whānau and communities,
- looking at industries that are especially important to Aotearoa New Zealand's overall wellbeing, including how global economic changes may affect them, and
- ensuring engagement with Māori, as well as other groups most greatly impacted, is central to identifying impacts and shaping responses.

Refresh Aotearoa New Zealand's Employment Strategy²⁸² to ensure it adequately considers the implications of the workforce disruptions anticipated by AI and new technologies, identifies and plans for any rapid response requirements for worst-case contingencies, and identifies relevant training or reskilling required to ensure all can participate in employment with opportunities to fulfil their needs and aspirations.

Support a rights-respecting technology sector

Support a rights-respecting technology sector by:

- incentivising AI development that benefits society,
- investigating digital competition and consumer protection reforms to address structural barriers that limit meaningful choice and alternatives in AI and digital services, and
- actively encouraging innovative ownership and governance models that recognise digital systems as shared infrastructure and support more equitable outcomes. This includes open-source infrastructure, public/state ownership, co-operatives, public-interest data trusts, and iwi-owned approaches.

Support Pacific data sovereignty

Evaluate what role Aotearoa New Zealand can play domestically and regionally in the promotion of Pacific data sovereignty,²⁸³ recognising the diversity of Pacific communities and countries, and the importance of data and digital empowerment to the rights of Pacific communities and nations.

System Enabler Two: Government leadership and accountability

The recommendations and first system enabler describe a whole-of-society undertaking built on the choices of empowered individuals and communities, supported by meaningful access, organised by a deliberate strategy, and operated by coordinated institutions. By contrast, there are some actions that only the Government can do, and the Government's accountability for doing them is a fundamental component of an effective human rights approach. Governments are the ultimate duty-bearers, required to act proactively to fulfil rights as well as to refrain from interfering with them.

The next two system enablers are about the Government taking accountability for its proactive obligations under human rights frameworks and Te Tiriti, and acting in the areas where only nation states can act. This includes establishing effective government accountability mechanisms and using the levers it has in the delivery of public services. It also includes ensuring appropriate regulatory interventions, which are covered in more detail in the next priority area.

Public sector actions are important in part because government procurement is a powerful lever for driving change. Public sector spending on digital systems shapes what is built, what is sold, and what is available to other purchasers and to the public. Procurement requirements that mandate interoperability, accessibility, data portability, and rights-respecting design can have direct effects across the wider market.

Practical Steps

Uphold Māori data sovereignty

Assess and develop strong accountability systems for how the public sector uses AI and digital technologies that recognise that, under Te Tiriti o Waitangi, Māori have rights over and in relation to their data. This means supporting iwi and hapū to exercise governance over their data in ways that fit their own priorities and approaches, which may differ across groups.

Ensure non-digital channels for essential public services

Ensure non-digital channels for essential public services are preserved as a matter of public service standard to the extent possible, and the closure of any non-digital channel requires a published rights-consistency assessment before it is made — particularly around participation requirements of the HRBA. This is especially important for older persons and those experiencing digital exclusion.

Recognise that people have a right to request a human decision-maker, and a right to seek human review of an automated decision. The HRBA requirements of transparency and accountability discussed above apply, particularly those involving the allocation of public funding, benefits, or services.

Require participatory engagement in design, deployment and evaluation of digital systems

Require participatory engagement in the design, deployment and evaluation of digital systems across the public sectors, and strengthen this over time by developing and promoting effective, rights-respecting methods for meaningful public input in line with the HRBA.

Embed rights-based public procurement

Review the Government Procurement Framework²⁸⁴ and Government Procurement Rules,²⁸⁵ and update them to adequately ensure the following considerations:

- Public-sector procurement of AI and digital technologies includes a mandatory human rights and Te Tiriti impact assessment as a condition of purchase. Māori data sovereignty should be a required component of this assessment and should be embedded in the licensing terms.
- Minimum procurement standards are ensured which cover interoperability, accessibility, auditability, and data governance.

Ensure accessible individual and collective complaints and accountability mechanisms

Establish clear, accessible and well-publicised pathways for individuals and communities to raise concerns or complaints about the use of AI and digital technologies where these may infringe on rights.

Ensure these mechanisms apply across both public and private sector use, and are supported by effective investigation and redress processes, including the ability to address collective and systemic harms, even if individual cases on their own might not trigger action.

Implement an algorithm register

Task responsible agencies to scope and implement a national register of algorithms used in the public sector, designed to promote transparency and accountability, drawing on work previously carried out.²⁸⁶ The register should be populated through existing processes (such as algorithm impact assessments) rather than requiring separate reporting, to reduce administrative burden and ensure consistency. This is in line with countries like the Netherlands and Canada among others.²⁸⁷

Establish AI harm reporting

Establish a national AI harm reporting and monitoring system, aligned with existing regulatory frameworks, to:

- enable proactive identification of risks and harms,
- encourage reporting through safe-harbour protections where appropriate, and
- support system-level learning and prevention.

Establish an AI safety institute

Establish or designate an independent body to function as an AI safety institute, responsible for providing technical evaluation and oversight of AI systems. This body should be technically-staffed and:

- offer independent, expert assessment of AI risks and impacts,
- be connected to the International Network of AI safety institutes²⁸⁸, and
- maintain a strong focus on addressing existing and emerging harms that affect rights, not solely long-term or frontier risks.

We note there are other examples of AI safety institutes internationally, and their role often includes conducting or sponsoring AI safety research and feeding the results into government decisions and international coordination.

System Enabler Three: Addressing legislative and regulatory gaps

In a domestic context, only Parliament can legislate. Designing legislation is difficult, but a human rights-based approach founded on Te Tiriti provides a layer of certainty, principle and agreement that supports more decisive action, as well as setting clear limitations.

As a first step the commission recommends resuming the regulatory review undertaken by the Department of Internal Affairs of online services and platforms, ‘Safer Online Services and Media Platforms Review’.²⁸⁹ This would build on the work which has already been done and identify regulatory and legislative gaps in this area, taking a rights-based approach to enhancing online safety through the review.²⁹⁰

In addition, the commission considers there are four immediate priorities for legislative action, which are outlined below. These practical steps aim to mitigate risks outlined above and ensure people’s rights are protected.

Practical Steps

Enforce rights to accessibility of digital systems

Efforts to accelerate the adoption of AI and digital systems throughout the public service and across Aotearoa New Zealand must be accompanied by efforts to ensure those systems do not exclude disabled people. Equally, government actions to require non-governmental entities to make their systems accessible are unlikely to be persuasive without the Government leading by example. Following advocacy by Access Matters Aotearoa, successive election cycles have seen commitments by MPs of all parties to make rights to accessibility legally enforceable,²⁹¹ but those promises have not been fulfilled.²⁹² Web accessibility standards are in place for the public service, but they are not enforceable in any meaningful way.²⁹³ As digital systems continue to expand beyond web pages, accessibility standards will also have to adapt.

Action: Implement an enforceable complaints and notification mechanism²⁹⁴ to systematically identify and remove barriers to accessibility for disabled people in digital environments, with real accountability for non-compliance. Where barriers cannot be removed, reasonable accommodations must be provided. Ensure that a proportionate approach is taken for private organisations, while ensuring that private sector entities are also subject to enforcement.

Address non-consensual sexual deepfakes

Non-consensual sexual deepfakes are the clearest case for immediate legislative action. At the moment, there is no legislation in force that makes it illegal to non-consensually share sexual imagery if these images were created by AI rather than through conventional photography, although a Bill is currently before the House that looks at this issue.²⁹⁵ Aotearoa New Zealand has so far failed to act on a documented harm that disproportionately affects women, takatāpui, and children,²⁹⁶ with no real suggestion of any protected interests preventing restrictions.

Action: Parliament should urgently enact legislation to prohibit the creation and distribution of non-consensual AI-generated sexual imagery, ensuring protections are equivalent to those applying to non-AI-generated content. Punitive actions should also be supplemented by AI literacy and education efforts. Preventative education should be focused on consent, respectful relationships, and safe online behaviour, including current and emerging risks associated with AI-enabled image-based abuse. Improvements should be made to the current Bill as per the commission’s submission to the Select Committee.²⁹⁷ In addition, the government should prohibit high-risk AI applications (such as “nudification” tools) that are designed, or readily capable, of facilitating image-based abuse, drawing on approaches taken in jurisdictions such as the EU, UK, and Australia.²⁹⁸

Strengthen transparency in public service use of automated systems

Section 22 of the Official Information Act gives people the right to access internal rules affecting decisions. It is the country's most under-used transparency lever, and its application to algorithmic decision rules is unresolved. Clarification by the Chief Ombudsman about what section 22 covers, with narrow legislative amendment if the issuance of guidance proves insufficient, would close that gap.

Action: The Chief Ombudsman should assess whether sections 22 and 23 of the Official Information Act 1982 apply to algorithmic systems used to inform decisions in respect of identifiable persons, and so issue guidance about how they should be applied. If the provisions are insufficient, Parliament should make a narrow amendment to section 22 of the Official Information Act and section 21 of the Local Government Official Information and Meetings Act 1987 to address any gaps.

Act on critical cyber infrastructure

Where the State digitises critical systems and requires people to use them to access essential services, it takes on a corresponding obligation to secure those systems. People cannot meaningfully exercise rights to health, social security, privacy, or participation in public life through infrastructure the State has made compulsory but has not adequately protected. Cybersecurity is therefore a precondition for the rights those systems influence, not an optional adjunct.

In May 2021 a ransomware attack on the Waikato District Health Board cut off access to clinical and administrative data, cancelled and delayed surgeries and appointments, took phone systems offline, and, in the words of the Government's own strategy, "threatened the lives of patients".²⁹⁹ In January 2026 the Office of the Privacy Commissioner opened an investigation into an alleged cybersecurity breach at Manage My Health, a patient portal holding the health records of around a quarter of the population. The High Court at Wellington granted an interim injunction restraining use of the stolen data.³⁰⁰ These are not isolated technical incidents. They are foreseeable harms to people whose access to healthcare depends on systems the State has encouraged or required them to use.

The New Zealand Cyber Security Strategy 2026–2030 recognises that "disruptions to critical infrastructure assets, systems, and networks have a debilitating effect on national security, economic performance, public health, and safety" and identifies strengthening the cybersecurity of critical infrastructure as a key priority.

Action: The Crown should recognise, in the next iteration of the Cyber Security Strategy³⁰¹ and in the development of any critical-infrastructure cyber-resilience regulatory regime, that securing critical cyber infrastructure is a human rights obligation, not solely a national security or economic issue. Where the government moves people onto digital channels to access essential public services — health, social security, education, and justice — it must ensure the security of those systems should be proportionate with the rights that depend on them.

Proportionate and decisive social media platform regulation

Around the world, and now in Aotearoa New Zealand, governments are proposing or acting on regulatory measures that ban social media companies from providing access to people under the age of 16. The evidence on whether these measures are effective is still emerging, though there is considerable indication that young people are using tools like Virtual Private Networks (VPNs) to access social media products

and services around these bans.³⁰² This has led to a corresponding suggestion that VPNs should be prohibited nationally,³⁰³ creating downstream impacts on anonymity and security for anyone who wants to connect to the Internet.³⁰⁴

A wide range of human rights bodies and institutions have emphasised that absolute social media bans on people under the age of 16 risk unjustifiably infringing rights to freedom of expression, and conclude there are more proportionate and effective measures available that would make these products and services safer for young people and everyone else.³⁰⁵

Action: Commit to a graduated and proportionate approach to platform regulation, grounded in a risk-based assessment of impacts on human rights, Te Tiriti o Waitangi and international best practice. This approach should be applied prior to implementing any restrictive measures on young people's access to digital platforms.

Social media bans for under-16s

In late 2024 and through 2025, several jurisdictions moved toward statutory restrictions on access to social media for people under 16 years of age: a ban came into force in Australia in December 2025, the United Kingdom government announced in June 2026 that similar measures are forthcoming, and France and other states are considering proposals. In Aotearoa New Zealand, both major political parties have indicated openness to action on online harms affecting young people; a Select Committee inquiry has reported; ministerial statements have flagged restrictions as an option; the Office of the Children's Commissioner, the Broadcasting Standards Authority, the Office of the Privacy Commissioner, and the Mental Health Foundation have variously engaged.

There is a real harm to address — algorithmic content systems, predatory contact, and the documented mental-health effects of certain platforms on certain young people. There is also a real cost. A blanket restriction interferes with rights of expression, association, and access to information under the Convention on the Rights of the Child. It interferes disproportionately with communities for whom online connection is a lifeline: trans and queer young people, and many young people in rural areas, and disabled young people whose social worlds are partly online, and young people in communities where the local cultural connection is not available in their immediate physical environment. The Māori population is demographically young, and a measure that targets young people necessarily targets Māori.

Implementation poses further questions. Age verification at the platform level requires identity infrastructure that itself engages privacy rights. VPNs allow people to get around age-related blocks, but banning these important security and privacy tools completely engages encryption and security interests for the wider population. A restriction that drives young people from regulated platforms to less safe environments produces a different harm. The Australian Human Rights Commission has published analysis of the human rights implications of Australia's social media ban for all Australians, including impacts on privacy, freedom of expression and digital rights.³⁰⁶

Scope liability for transnational technology companies

Aside from social media companies, a range of other companies that operate digital products and services have human rights obligations in Aotearoa New Zealand as they do in other jurisdictions, including those outlined in the UNGPs. AI companies and others already operate in jurisdictions with stronger human rights protections, and should therefore be prepared to honour those obligations here too. The commission recognises that this presents complex legal issues, but urges companies and governments to explicitly recognise the private sector's human rights obligations and to identify measures that would strengthen accountability for honouring those obligations.

Action: Scope meaningful liability and enforcement mechanisms for transnational technology companies operating in Aotearoa New Zealand.

Address consumer device ambient surveillance

Consumer device ambient surveillance with data collection through products like smart glasses, AI pins, AirPods with cameras, and in-vehicle microphones is arriving in force. This creates issues for privacy, social cohesion, data sovereignty, public participation, and has a range of associated consequences. However, smart devices can also play a powerful enabling role, particularly where they can enhance accessibility for disabled people.

Action: Undertake a proactive, technology-neutral review of consumer device ambient surveillance, reflecting that such devices are on sale already and increasing in number, to ensure that existing data protections are appropriate and will uphold human rights and Te Tiriti o Waitangi. A human rights-based approach must be adopted in this review, which recognises in particular that disabled people may genuinely rely on such devices to realise other human rights, that unjustifiable steps to arbitrarily limit access to or use of these devices may not be defensible, and that proportionate measures like registration or education schemes may be more appropriate. Devices that should be in scope include smart glasses, AI pins, AirPods with cameras, AR and VR head-mounted displays, smart-home devices, and in-vehicle microphones.

Appendix One: Engagement to support the development of this report

This paper was informed by insights shared by those listed below. We thank them for their generosity and thoughtful contributions. Responsibility for the content of the paper including the analysis, conclusions, and any errors, rests solely with the commission.

Expert Advisory Group members

Te Kou Rikirangi Gage, Te Kāhui Raraunga Trust

Dr Karaitiana Taiuru, Director, Institute of AI Governance

Professor Te Taka Keegan, Co-Director Māori, Artificial Intelligence Institute, University of Waikato

Dr Andrew Chen, Technology Ethics Researcher, Honorary Research Associate, Complex Conversations Lab, University of Auckland

Emma MacDonald, Director, Centre for Data Ethics and Innovation, Stats NZ

Julia Arnott-Neenee, Co-Founder and CEO, Fibre Fale

Dr Yun Sing Koh, Professor at the School of Computer Science, University of Auckland

Anjum Rahman, Founder and Facilitator, Tāhono Trust

Ari, Project Lead – Belonging & Inclusion, Tāhono Trust

Tim Young, Chief Executive Officer of Smart Access Ltd and Chief Technology Officer at My Life My Voice

Maya Pan, Director, Redwood Pan Group

Independent reviewers

Professor Alexandra Andhov, Chair in Law and Technology, Director of Centre for Advancing Law and Technology Responsibly, University of Auckland

Professor Ali Knott, School of Engineering and Computer Science, Victoria University of Wellington

Professor Hēmi Whaanga, Head of School, Te Pūtahi-a-Toi, School of Māori Knowledge

Other experts and agencies consulted

Peter-Lucas Jones, Te Hiku Media

Karolina Iwanska, European Centre for Non-Profit Law

Dr Andrew Lensen, Victoria University of Wellington

Caroline Flora, Classification Office

Dr Cassandra Mudgway, University of Canterbury

Professor Edward Santow, UTS Human Technology Institute

Erena Mikaere, Te Kāhui Raraunga

Dr John Flackett, AiLab

Joy Liddicoat, Research Affiliate, University of Otago

Kirikowhai Mikaere, Te Kāhui Raraunga

Dr Lorraine Finlay, Australian Human Rights Commission

Madeline Newman, AI Forum New Zealand | Te Kāhui Atamai Iahiko o Aotearoa

Namulau'ulu Nu'uali'i Eteroa Lafaele, Fibre Fale

Shannon Novak, AISF (Artificial Intelligence Safety Forum)

Liam Williams, Ministry of Business, Innovation & Employment

Michael Webster, Privacy Commissioner

Mana Mokopuna, Children's Commissioner

Tom Barraclough, Brainbox

Ellen Strickland, Brainbox

Appendix Two: AI methodology

Some of the initial underlying research, analysis and drafting for this report was supported by AI, under human direction. The accountable person for the use of AI in this project is Tom Barraclough at the Brainbox Institute.

The research and drafting for this report drew on a large body of source material — international human rights instruments and authoritative interpretations, Aotearoa New Zealand law and policy, comparator regulation from other jurisdictions, civil society and academic research, and stakeholder input from the Expert Advisory Group and the wider engagement programme. AI tools were used to maintain systematic coverage of that material, to search and analyse it against a known and bounded corpus rather than free-associating from a model’s training, and to produce drafts that human reviewers then revised against stakeholder input and the deliberations of the Expert Advisory Group. The judgement at every step — what a source means, what matters, how the passages fit together, and what the commission considers — stayed with the human authors. Stakeholder material identified as sensitive was processed locally and was not transmitted to remote services. Material subject to particular sensitivity from the perspective of Māori data sovereignty was handled separately.

The methodology was designed from the outset to be inspectable. Source documents were converted to clean, structured text and held under version control alongside the indexes, working notes, and drafts the research produced. Each substantive topic in the report left a trail of linked artefacts — source, index, working note, and drafted passage — so that the path from a sentence in the report back to the material behind it can be traced.

End Notes

- ¹ New Zealand Government Chief Digital Officer, “Glossary of AI Terms,” 2025, <https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/artificial-intelligence/responsible-ai-guidance-for-the-public-service-genai/glossary-of-ai-terms>, quoting and attributing to the OECD the definition: “An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or isions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.”
- ² Organisation for Economic Co-operation and Development (OECD), Explanatory Memorandum on the Updated OECD Definition of an AI System, OECD Artificial Intelligence Papers No. 8 (Paris: OECD Publishing, March 2024), DSTI/CDEP/AIGO(2023)8/FINAL, https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/03/explanatory-memorandum-on-the-updated-oecd-definition-of-an-ai-system_3c815e51/623da898-en.pdf.
- ³ See Nicole Gillespie et al., “Key Findings on Public Attitudes Towards AI,” Melbourne Business School, The University of Melbourne and KPMG, 2025, <https://mbs.edu/faculty-and-research/trust-and-ai/key-findings-on-public-attitudes-towards-AI>; Ipsos, Public Trust in AI: Implications for Policy and Regulation (Ipsos Public Affairs UK, September 2024), <https://www.ipsos.com/sites/default/files/ct/news/documents/2024-09/Ipsos%20Public%20Trust%20in%20AI.pdf>; similar findings in the USA, see Colleen McClain et al., “How the U.S. Public and AI Experts View Artificial Intelligence,” Pew Research Center, April 3, 2025, <https://www.pewresearch.org/internet/2025/04/03/how-the-us-public-and-ai-experts-view-artificial-intelligence/>
- ⁴ Nicole Gillespie, Steven Lockey, Tabi Ward, Alexandria Macdade, and Gerard Hassed, Trust, Attitudes and Use of Artificial Intelligence: A Global Study 2025 (The University of Melbourne and KPMG, 2025), 32, <https://doi.org/10.26188/28822919>. The study identifies what best predicts trust in AI and finds responsible AI governance to be by far the biggest predictor — almost three times larger than any other predictor (including ‘motivational: benefits’, ‘knowledge: AI literacy’ and ‘uncertainty: risks’)
- ⁵ AI Forum New Zealand, AI Blueprint for Aotearoa (AI Forum New Zealand, May 2026), <https://aiforum.org.nz/2026/05/06/ai-blueprint-for-aotearoa-a-refreshed-vision-to-2030/>.
- ⁶ Digital Equity Coalition Aotearoa (DECA), A Fair Chance for All: Breaking the Cycle of Persistent Disadvantage (Submission to the New Zealand Productivity Commission, November 11, 2022), <https://www.treasury.govt.nz/sites/default/files/2024-05/pc-inq-fcfa-dr-136-digital-equity-coalition-aotearoa.pdf>
- ⁷ Ibid.
- ⁸ Verian, for InternetNZ Ipurangi Aotearoa, New Zealand’s Internet Insights: 2025 Survey Findings (InternetNZ Ipurangi Aotearoa, 2025), <https://internetnz.nz/assets/Archives/New-Zealands-Internet-Insights-2025-survey-findings.pdf>.
- ⁹ Ibid.
- ¹⁰ See more under the duty to respect, protect, and fulfil human rights.
- ¹¹ United Nations Office of the United Nations High Commissioner for Human Rights (OHCHR), *Mapping Report: Human Rights and New and Emerging Digital Technologies*, UN Doc A/HRC/56/45 (2024), para 61, <https://undocs.org/A/HRC/56/45>.
- ¹² New Zealand House of Representatives, Education and Workforce Committee, *Inquiry into the Harm Young New Zealanders Encounter Online, and the Roles That Government, Business, and Society Should Play in Addressing Those Harms: Final Report* (54th Parliament, March 2026), <https://selectcommittees.parliament.nz/view/SelectCommitteeReport/51deb7d3-6f4c-48bb-8a93-08de7a2437b3>.

- ¹³ Hon Judith Collins, *Driving Down the Cost of Digital in Government – Implementation* (Cabinet paper; Cabinet Minute ECO-25-MIN-0217 and Cabinet Minute CAB-25-MIN-0476, Public Service Commission, 2026), <https://www.publicservice.govt.nz/assets/DirectoryFile/Driving-down-the-cost-of-digital-in-government-Implementation.pdf>.
- ¹⁴ Nicola Willis and Paul Goldsmith, “Public Service to Be Overhauled,” Beehive.govt.nz, May 19, 2026, <https://www.beehive.govt.nz/release/public-service-be-overhauled>.
- ¹⁵ Human Rights Act 1993 (NZ), s 5(1)(a) <https://www.legislation.govt.nz/act/public/1993/82/en/latest/#DLM304212>; The commission’s mandate also includes advocating for human rights and promoting and protecting the observance of human rights through education and public awareness (s 5(2)(a)); promoting, by research, education, and discussion, a better understanding of the human rights dimensions of the Treaty of Waitangi and their relationship with domestic and international human rights law (s 5(2)(d)); receiving and inviting representations from members of the public on matters affecting human rights (s 5(2)(f)); and promoting and monitoring compliance with international human rights instruments (s 5(2)(kc)).
- ¹⁶ The two examples are the Australian Robodebt scheme and the Netherlands childcare-benefits scandal (Toeslagenaffaire). On Robodebt, see Royal Commission into the Robodebt Scheme (Commissioner Catherine Holmes AC SC), Report of the Royal Commission into the Robodebt Scheme (Canberra: Commonwealth of Australia, 2023), <https://robodebt.royalcommission.gov.au/publications/report>. On the Netherlands scandal, see Melissa Heikkilä, “Dutch Scandal Serves as a Warning for Europe over Risks of Using Algorithms,” *POLITICO*, March 29, 2022, <https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/>; and Amnesty International, *Xenophobic Machines: Discrimination through Unregulated Use of Algorithms in the Dutch Childcare Benefits Scandal* (London: Amnesty International, 2021), <https://www.amnesty.org/en/documents/eur35/4686/2021/en/>.
- ¹⁷ This definition is also used in the New Zealand Government’s AI strategy: Ministry of Business, Innovation and Employment (MBIE), *New Zealand’s Strategy for Artificial Intelligence: Investing with Confidence* (Wellington: MBIE, 2025), <https://www.mbie.govt.nz/assets/new-zealands-strategy-for-artificial-intelligence.pdf>. It is also embedded in the European Union AI Act, Regulation (EU) 2024/1689 of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), art 3(1); and in the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, art 2 (the same definition, and its use in the EU AI Act, is confirmed in Council of Europe, *Handbook on Human Rights and Artificial Intelligence*, Handbook of the Steering Committee for Human Rights (CDDH), PREMS 055926 (Strasbourg: Council of Europe, 2026), noting that ‘this definition is also used in the EU AI Act, Article 3 § 1.’).
- ¹⁸ Organisation for Economic Co-operation and Development (OECD), *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449 (2024, as amended), <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>; definition quoted verbatim in OECD, *Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions* (Paris: OECD Publishing, 2025).
- ¹⁹ Organisation for Economic Co-operation and Development (OECD), *Explanatory Memorandum on the Updated OECD Definition of an AI System*, prepared by Karine Perset et al., OECD Artificial Intelligence Papers, No. 8 (Paris: OECD Publishing, March 2024), Doc. DSTI/CDEP/AIGO(2023)8/FINAL, https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/03/explanatory-memorandum-on-the-updated-oecd-definition-of-an-ai-system_3c815e51/623da898-en.pdf.
- ²⁰ Ministry of Business, Innovation and Employment (MBIE), *Responsible AI Guidance for Businesses* (Wellington: MBIE, July 2025), ISBN 978-1-99-106999-3 (online).
- ²¹ Billy Perrigo, “Exclusive: OpenAI Used Kenyan Workers on Less Than \$2 Per Hour to Make ChatGPT Less Toxic,” *TIME*, January 18, 2023, <https://time.com/6247678/openai-chatgpt-kenya-workers/>.
- ²² Stats NZ, “Algorithm Charter for Aotearoa New Zealand,” data.govt.nz, 2020, last reviewed June 15, 2023, <https://data.govt.nz/toolkit/data-ethics/government-algorithm-transparency-and-accountability/algorithm-charter>.

- ²³ For an introduction to this stack, see Francesca Bria, Paul Timmers, and Fausto Gernone, “EuroStack,” euro-stack.info, 2025, <https://www.euro-stack.info/>.
- ²⁴ Peter Slattery et al., “The AI Risk Repository: A Meta-Review, Database, and Taxonomy of Risks from Artificial Intelligence,” *Patterns* (Cell Press), 2026, <https://doi.org/10.1016/j.patter.2026.101517>. The paper systematically analysed 74 AI-risk frameworks containing 1,725 distinct risks and found that human decisions account for 38% of AI risks and AI systems themselves for 42%.
- ²⁵ Te Kāhui Raraunga, *Māori AI Governance: A Framework for Ethical Governance of AI in Aotearoa* (Te Kāhui Raraunga, 2025), https://www.kahuiraraunga.io/_files/ugd/b8e45c79f4162207da4123861c50dec08cd0fb.pdf. Recommendation 2, <https://www.kahuiraraunga.io/maoriaigovernance>. The Framework requires that algorithmic systems be accompanied by documentation of their whakapapa — tracing lineage back through datasets, including synthetic data, to the original information.
- ²⁶ Jeroen van den Hoven, “The Design Turn in Applied Ethics,” in *Designing in Ethics*, ed. Jeroen van den Hoven, Seumas Miller, and Thomas Pogge (Cambridge University Press, 2017), 11–31, <https://doi.org/10.1017/9780511844317.002>.
- ²⁷ Waitangi Tribunal, *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, Lower Hutt: Legislation Direct, 2014), https://forms.justice.govt.nz/search/Documents/WT/wt_DOC_85648980/Te%20RakiW_1.pdf.
- ²⁸ *Te Pou Matakana Limited v Attorney-General* [2021] NZHC 3319.
- ²⁹ Privacy Act 2020 (NZ), ss 21(a) and 22 <https://www.legislation.govt.nz/act/public/2020/31/en/latest/#LMS23223>
- ³⁰ MBIE, *Responsible AI Guidance for Businesses*, see note 20 above, “Governance and Accountability” section.
- ³¹ Countries including Australia, Canada, Japan, the United Kingdom, the United States, Israel, Argentina, Costa Rica, Peru, and Uruguay have supported the creation of a binding international framework for AI governance through their participation in the negotiation and/or signature of the Council of Europe Framework Convention on Artificial Intelligence, the world’s first legally binding international AI treaty see Council of Europe, *The Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (September 2024), <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence> ; Council of Europe, *Council of Europe Opens First Ever Global Treaty on AI for Signature*, September 5, 2024, <https://www.coe.int/en/web/portal/-/council-of-europe-opens-first-ever-global-treaty-on-ai-for-signature>
- ³² Lindsey Andersen, *Human Rights in the Age of Artificial Intelligence* (Access Now, 2018), <https://www.accessnow.org/wp-content/uploads/2018/11/AI-and-Human-Rights.pdf>.
- ³³ United Nations General Assembly, *Seizing the Opportunities of Safe, Secure and Trustworthy Artificial Intelligence Systems for Sustainable Development*, UN Doc A/RES/78/265 (2024), para 5, <https://undocs.org/A/RES/78/265>.
- ³⁴ United Nations General Assembly, *Universal Declaration of Human Rights*, UN Doc A/RES/217 A (III) (1948), <https://www.un.org/en/about-us/universal-declaration-of-human-rights>.
- ³⁵ United Nations General Assembly, *International Covenant on Civil and Political Rights*, UN Doc A/RES/2200A (XXI) (1966), <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>.
- ³⁶ United Nations General Assembly, *International Covenant on Economic, Social and Cultural Rights*, UN Doc A/RES/2200A (XXI) (1966), <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights>.
- ³⁷ The United Nations considers that there are 9 core human rights treaties however two of these have not been ratified by New Zealand, this number also does not include the optional protocols see <https://www.ohchr.org/en/core-international-human-rights-instruments-and-their-monitoring-bodies>

- ³⁸ United Nations General Assembly, *International Convention on the Elimination of All Forms of Racial Discrimination*, UN Doc A/RES/2106 (XX) (1965), <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-elimination-all-forms-racial>.
- ³⁹ United Nations General Assembly, *Convention on the Elimination of All Forms of Discrimination against Women*, UN General Assembly Resolution 34/180 (18 December 1979), entered into force 3 September 1981, <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-elimination-all-forms-discrimination-against-women>.
- ⁴⁰ *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*, opened for signature 10 December 1984, 1465 UNTS 85 (entered into force 26 June 1987).
- ⁴¹ United Nations General Assembly, *Convention on the Rights of the Child*, UN General Assembly Resolution 44/25 (20 November 1989), entered into force 2 September 1990, <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child>.
- ⁴² United Nations General Assembly, *Convention on the Rights of Persons with Disabilities*, UN General Assembly Resolution A/RES/61/106 (12 December 2006), entered into force 3 May 2008, <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-persons-disabilities>.
- ⁴³ *Convention for the Protection of Human Rights and Fundamental Freedoms* (European Convention on Human Rights), November 4, 1950, ETS No. 5, <https://www.echr.coe.int/european-convention-on-human-rights>.
- ⁴⁴ European Commission, “European Declaration on Digital Rights and Principles,” *Shaping Europe’s Digital Future*, December 15, 2022, <https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles>.
- ⁴⁵ Other international sources refer to, for example: Organisation for Economic Co-operation and Development (OECD) guidance; Commentary and guidance from other United Nations bodies such as the Office of the High Commissioner for Human Rights or World Health Organisation, United Nations Treaty Body General Comments and Jurisprudence or reports of UN independent experts.
- ⁴⁶ United Nations General Assembly, *United Nations Declaration on the Rights of Indigenous Peoples* (UNDRIP), UN Doc A/RES/61/295 (2007) UNDRIP was adopted by the UN General Assembly and endorsed by New Zealand in 2010. In practice, UN committees, special rapporteurs, and international courts routinely rely on UNDRIP when interpreting binding instruments. It carries with it significant international, political and normative authority.
- ⁴⁷ [2021] NZHC 3319
- ⁴⁸ Australian Human Rights Commission, “Human Rights-Based Approaches,” *Rights and Freedoms*, June 18, 2013, <https://humanrights.gov.au/resource-hub/by-resource-type/articles/rights-and-freedoms/human-rights-based-approaches>.
- ⁴⁹ Virginia Dignum, Rachele Carli, and Tang Yingxia, *Background Paper: Human Rights & Artificial Intelligence* (background paper prepared for the 23rd Informal ASEM Seminar on Human Rights, 29–31 October 2025, Asia-Europe Foundation and Raoul Wallenberg Institute of Human Rights and Humanitarian Law, 2025), 6.
- ⁵⁰ Australian Human Rights Commission, *Human Rights and Technology Final Report: Summary* (ISBN 978-1-925917-34-5, Sydney: Australian Human Rights Commission, 2021), 11, https://humanrights.gov.au/data/assets/file/0025/46933/Ahrc_rightstech_2021_final_summary_1.pdf
- ⁵¹ Dignum et al, *Background Paper: Human Rights & Artificial Intelligence*, see note 49 above, 6.
- ⁵² United Nations General Assembly, Resolution 78/265, “Seizing the Opportunities of Safe, Secure and Trustworthy Artificial Intelligence Systems for Sustainable Development,” UN Doc A/RES/78/265 (21 March 2024); also see OECD, “Human Rights in the Digital Age,” OECD, <https://www.oecd.org/en/topics/sub-issues/human-rights-in-the-digital-age.html>.

- ⁵³ See David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/73/348 (29 August 2018); Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/48/31 (13 September 2021); Maria Paz Canales et al., “What Would a Human Rights-Based Approach to AI Governance Look Like?,” *Global Partners Digital* (blog), September 19, 2023, <https://www.gp-digital.org/what-would-a-human-rights-based-approach-to-ai-governance-look-like/>; BSR, *Fundamentals of a Human Rights-Based Approach to Generative AI* (BSR, n.d.), <https://www.bsr.org/files/BSR-Fundamentals-of-a-Human-Rights-Based-Approach-to-Generative-AI.pdf>; Digital Cooperation Organization, *Rights by Design: Embedding Human Rights Principles in AI Systems* (Digital Cooperation Organization, 2025), <https://dco.org/wp-content/uploads/2025/06/Rights-by-Design-Embedding-Human-Rights-Principles-on-AI-systems.pdf>; International Commission of Jurists, *Digital Technologies and Human Rights: A Legal Framework*, Briefing Paper (Geneva: International Commission of Jurists, May 2022), <https://www.icj.org/wp-content/uploads/2022/05/Digital-Technologies-and-Human-Rights-Briefing-Paper-FINAL-VERSION-May-2022.pdf>.
- ⁵⁴ See Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, 2015); OECD, *Artificial Intelligence in Society* (OECD, 2019), <https://www.oecd.org/going-digital/ai-in-society/>; Jenna Burrell, “How the Machine ‘Thinks’: Understanding Opacity in Machine Learning Algorithms,” *Big Data & Society* 3, no. 1 (2016), <https://doi.org/10.1177/2053951715622512>.
- ⁵⁵ See UNESCO, “Recommendation on the Ethics of Artificial Intelligence,” UNESCO, May 16, 2023, <https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence>; Office of the United Nations High Commissioner for Human Rights, “Office of the United Nations High Commissioner for Human Rights (OHCHR),” AI for Good, International Telecommunication Union, accessed May 17, 2026, <https://aiforgood.itu.int/about-us/un-ai-actions/ohchr/>.
- ⁵⁶ See Alessandro Mantelero, “AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment,” *Computer Law & Security Review* 34, no. 4 (2018): 754–772, <https://doi.org/10.1016/j.clsr.2018.05.017>; Lorna McGregor, Daragh Murray, and Vivian Ng, “International Human Rights Law as a Framework for Algorithmic Accountability,” *International & Comparative Law Quarterly* 68, no. 2 (2019): 309–343, <https://doi.org/10.1017/S0020589319000046>.
- ⁵⁷ See Information Commissioner’s Office (UK) and The Alan Turing Institute, “Explaining Decisions Made with AI,” Information Commissioner’s Office, 2020, <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-ai/>; Ben Chester Cheong, “Transparency and Accountability in AI Systems: Safeguarding Wellbeing in the Age of Algorithmic Decision-Making,” *Frontiers in Human Dynamics* 6 (2024), published July 2, 2024, <https://doi.org/10.3389/fhumd.2024.1421273>.
- ⁵⁸ See OECD, “AI Principles” (Principle 1.5, Accountability), OECD, adopted 2019, updated 2024, <https://www.oecd.org/en/topics/ai-principles.html>; European Commission High-Level Expert Group on Artificial Intelligence, “Ethics Guidelines for Trustworthy AI,” European Commission, April 8, 2019, <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>; Information Commissioner’s Office (UK) and The Alan Turing Institute, “Explaining Decisions Made with AI,” 2020, <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-ai/>; UN General Assembly, Report of the Special Rapporteur on Extreme Poverty and Human Rights, UN Doc A/74/48037 (2019), <https://undocs.org/A/74/48037>.
- ⁵⁹ See Office of the United Nations High Commissioner for Human Rights (OHCHR), “Description of Activities on AI,” AI for Good (International Telecommunication Union), accessed July 14, 2026, <https://aiforgood.itu.int/about-us/un-ai-actions/ohchr/>.
- ⁶⁰ Vithya Yogarajan, Gillian Dobbie, Te Taka Keegan, and Rostam J. Neuwirth, “Tackling Bias in Pre-trained Language Models: Current Trends and Under-represented Societies,” arXiv, December 3, 2023, <https://arxiv.org/abs/2312.01509>; and Te Taka Keegan, personal communication, June 26, 2026.

- ⁶¹ See United Nations Sustainable Development Group, Human Rights-Based Approach, accessed July 17, 2026, <https://unsdg.un.org/2030-agenda/universal-values/human-rights-based-approach>; Office of the United Nations High Commissioner for Human Rights, International Human Rights Law, accessed July 17, 2026, <https://www.ohchr.org/en/instruments-and-mechanisms/international-human-rights-law>; Office of the United Nations High Commissioner for Human Rights, International Covenant on Civil and Political Rights, accessed July 17, 2026, <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-right>; United Nations Sustainable Development Group, Human Rights-Based Approach.
- ⁶² Ibid.
- ⁶³ UNDRIP see note 46 above Article 3.
- ⁶⁴ The right to self-determination is also included in common Article 1 (1) of ICCPR and ICESCR which are binding on Aotearoa New Zealand.
- ⁶⁵ Te Puni Kōkiri, “UN Declaration on the Rights of Indigenous Peoples,” accessed July 23, 2026, <https://www.tpk.govt.nz/en/a-matou-whakaarotau/te-ao-maori/un-declaration-on-the-rights-of-indigenous-peoples>; Te Kāhui Tika Tangata Human Rights Commission, “Monitoring the Declaration on the Rights of Indigenous Peoples,” April 27, 2023, <https://tikatangata.org.nz/our-work/monitoring-the-declaration-on-the-rights-of-indigenous-peoples-2>
- ⁶⁶ UNDRIP see note 46 above, Article 29.
- ⁶⁷ Vithya Yogarajan, Gillian Dobbie, Te Taka Keegan, and Rostam J. Neuwirth, “Tackling Bias in Pre-trained Language Models: Current Trends and Under-represented Societies,” arXiv, December 3, 2023, <https://arxiv.org/abs/2312.01509>.
- ⁶⁸ Te Kāhui Raraunga, *Māori AI Governance: A Framework for Ethical Governance of AI in Aotearoa* 25.
- ⁶⁹ First International Conference on the Cultural and Intellectual Property Rights of Indigenous Peoples, *Mataatua Declaration on Cultural and Intellectual Property Rights of Indigenous Peoples* (Whakatane, Aotearoa New Zealand, 12–18 June 1993), UN Doc E/CN.4/Sub.2/AC.4/1993/CRP.5 (Geneva, 26 July 1993), <https://digitallibrary.un.org/record/170882?ln=en>.
- ⁷⁰ United Nations General Assembly, *United Nations Declaration on the Rights of Indigenous Peoples*, UN Doc A/RES/61/295 (13 September 2007), arts 19, 31; see also Karaitiana Taiuru, “Māori Data Sovereignty and Digital Colonisation,” accessed July 14, 2026, <https://www.taiuru.maori.nz/maori-data-sovereignty-and-digital-colonisation/>
- ⁷¹ *Te Pou Matakana Ltd v Attorney-General* [2021] NZHC 3319.
- ⁷² New Zealand Waitangi Tribunal, *Ko Aotearoa Tēnei: A Report into Claims Concerning New Zealand Law and Policy Affecting Māori Culture and Identity, Te Taumata Tuatahi* (WAI 262, Wellington: Legislation Direct, 2011).
- ⁷³ Te Mana Raraunga (Māori Data Sovereignty Network), “Frequently Asked Questions (Pātai),” accessed July 14, 2026, <https://www.temanararaunga.maori.nz/patai>.
- ⁷⁴ Tahu Kukutai et al., *Māori Data Governance Model* (Te Kāhui Raraunga, 2023), <https://www.kahuiraraunga.io/maoridatagovernance>.
- ⁷⁵ Te Mana Raraunga (Māori Data Sovereignty Network), “Our Data, Our Sovereignty, Our Future,” Te Mana Raraunga, accessed July 14, 2026, <https://www.temanararaunga.maori.nz/>.
- ⁷⁶ Te Kāhui Raraunga, *Māori AI Governance: A Framework for Ethical Governance of AI in Aotearoa* see note 25 above; Tahu Kukutai et al., *Māori Data Governance Model*, ibid.
- ⁷⁷ Te Mana Raraunga (Māori Data Sovereignty Network), *Principles of Māori Data Sovereignty*, TMR Brief No. 1 (October 2018), <https://www.temanararaunga.maori.nz/s/TMR-Maori-Data-Sovereignty-Principles-Oct-2018.pdf>.

- ⁷⁸ Global Indigenous Data Alliance (GIDA), “The CARE Principles for Indigenous Data Governance,” GIDA, accessed July 14, 2026, <https://www.gida-global.org/careprinciples>. The principles were drafted at the International Data Week and Research Data Alliance Plenary co-hosted workshop, “Indigenous Data Sovereignty Principles for the Governance of Indigenous Data,” 8 November 2018, Gaborone, Botswana, co-led by Stephanie Russo Carroll and Maui Hudson.
- ⁷⁹ Te Taka Keegan, personal communication, June 26, 2026.
- ⁸⁰ Te Mana Raraunga, *Principles of Māori Data Sovereignty*, see note 77 above.
- ⁸¹ Tahu Kukutai et al., *Māori Data Governance Model*, see note 74 above.
- ⁸² Te Kāhui Raraunga, *Māori AI Governance: A Framework for Ethical Governance of AI in Aotearoa* see note 25 above.
- ⁸³ Karaitiana Taiuru, “Māori Data Governance Report,” *Te Kete o Karaitiana Taiuru* (blog), August 28, 2025, <https://www.taiuru.co.nz/maori-data-governance-in-2025/>.
- ⁸⁴ Karaitiana Taiuru, “6 Te Tiriti Based Artificial Intelligence Ethical Principles,” *Te Kete o Karaitiana Taiuru* (blog), October 27, 2023, <https://www.taiuru.co.nz/ai-principles/>.
- ⁸⁵ Karaitiana Taiuru, personal communication, April, 2026.
- ⁸⁶ Pacific Data Sovereignty Trust, “About Us,” accessed July 14, 2026, <https://pacificdatasovereignty.com/about-us-2/>.
- ⁸⁷ International Convention on the Elimination of All Forms of Racial Discrimination (CERD) (1965); Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) (1979); Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT) (1984); Convention on the Rights of the Child (UNCROC) (1989) and Convention on the Rights of Persons with Disabilities (CRPD) (2006).
- ⁸⁸ UN Treaty bodies oversee the implementation of each treaty and provide authoritative guidance on the rights contained within the treaty and their implementation in its published General Comments or general recommendations.
- ⁸⁹ Office of the United Nations High Commissioner for Human Rights, “B-Tech Project,” OHCHR, accessed March 15, 2026, <https://www.ohchr.org/en/business-and-human-rights/b-tech-project>.
- ⁹⁰ Office of the United Nations High Commissioner for Human Rights, *Mapping Report: Human Rights and New and Emerging Digital Technologies*, UN Doc A/HRC/56/45 (2024), <https://undocs.org/A/HRC/56/45>.
- ⁹¹ Yoshua Bengio et al., *International AI Safety Report 2026* (DSIT 2026/001; London: UK Department for Science, Innovation and Technology, 2026), <https://internationalaisafetyreport.org/publication/international-ai-safety-report-2026>.
- ⁹² For more information on the right see OHCHR, *The Right to Privacy in the Digital Age*, see note 53 above; Office of the United Nations High Commissioner for Human Rights, “Special Rapporteur on the Right to Privacy,” OHCHR, accessed July 14, 2026, <https://www.ohchr.org/en/special-procedures/sr-privacy>; and Ineta Ziemele, “Privacy, Right to, International Protection,” in *Max Planck Encyclopedia of Public International Law*, ed. Anne Peters and Rüdiger Wolfrum (Oxford University Press), last updated March 2009, <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e863?p=emailAk71gyt66GCdo&d=/10.1093/law:epil/9780199231690/law-9780199231690-e863&print>.
- ⁹³ *Hosking v Runting* [2005] 1 NZLR 1 (CA).
- ⁹⁴ International Covenant on Civil and Political Rights, art 2; International Covenant on Economic, Social and Cultural Rights, art 2.
- ⁹⁵ Office of the Privacy Commissioner, *Inquiry into Foodstuffs North Island Trial Use of Facial Recognition Technology* (Wellington: Office of the Privacy Commissioner, 2025), <https://www.privacy.org.nz/focus-areas/frt-inquiry-report/>. FSNi is a separate co-operative from FSSI; its six-month trial across twenty-five New World and PAK’nSAVE stores ran 8 February–7 September 2024, and the report — released 4 June 2025 — found the trial compliant while setting expectations for future use.

- ⁹⁶ *Biometric Processing Privacy Code 2025* (New Zealand), New Zealand Gazette notice 2025-sl4213, issued 21 July 2025, in force 3 November 2025, <https://gazette.govt.nz/notice/id/2025-sl4213>. The Code substitutes thirteen biometric-specific rules for the Information Privacy Principles; agencies already processing biometric information before 3 November 2025 have until 3 August 2026 to comply.
- ⁹⁷ FSSI's pilot concluded in January 2026 and is documented in a Privacy Impact Assessment prepared under the Code: Foodstuffs South Island, *Facial Recognition Technology: Privacy Impact Assessment* (Foodstuffs South Island, 2026), 6–8, 13, https://au-assets.contentstack.com/v3/assets/blteb34c6547156cbf3/blt279bcd2081615322/6a20ef1e1eefafdeacd27219/Foodstuffs_South_Island_Privacy_Impact_Assessment.pdf; see also Foodstuffs South Island, “Facial Recognition,” January 2026, <https://www.foodstuffs-si.co.nz/news-room/Facial-recognition>. The Māori Data Governance Model — developed by Māori data experts under the mandate of the Data Iwi Leaders Group and Te Kāhui Raraunga, organised around eight pou, and designed for the public service — is set out in Tahu Kukutai et al., *Māori Data Governance Model* (Te Kāhui see note 76 above. Per the PIA, FSSI states it engages each pou; in practice a retail deployment leans most on Pou 4 (data protection), 7 (quality and system integrity) and 8 (classification). Watchlist enrolment excludes minors and vulnerable people (8); the misidentification process is aligned with tikanga, including tapu, mana, mauri, hau and utu (13).
- ⁹⁸ As they apply to Aotearoa New Zealand, for example the Convention on Enforced Disappearances is not included as Aotearoa New Zealand has not ratified this Treaty.
- ⁹⁹ See Expert Mechanism on the Right to Development (OHCHR), “Artificial Intelligence, Cultural Rights, and the Right to Development — Thematic Study by the Expert Mechanism on the Right to Development,” OHCHR, published 13 April 2026, <https://www.ohchr.org/en/documents/ongoing-studies/artificial-intelligence-cultural-rights-and-right-development-thematic>.
- ¹⁰⁰ Committee on Economic, Social and Cultural Rights, General Comment No. 25 (2020) on Science and Economic, Social and Cultural Rights (Article 15 (1)(b), (2), (3) and (4) of the International Covenant on Economic, Social and Cultural Rights), <https://docs.un.org/en/E/C.12/GC/25> (30 April 2020).
- ¹⁰¹ *Ibid.*
- ¹⁰² *Ibid.*, para 52.
- ¹⁰³ *Ibid.*, para 75.
- ¹⁰⁴ *Ibid.*, paras 75–76; also see UN Special Rapporteur on Extreme Poverty and Human Rights (Philip Alston), Report on Extreme Poverty and Human Rights (Digital Welfare States and Human Rights), UN Doc A/74/493 (2019), <https://www.ohchr.org/en/documents/thematic-reports/a74493-digital-welfare-states-and-human-rights-report-special-rapporteur>.
- ¹⁰⁵ Aotearoa New Zealand ratified the International Covenant on Economic, Social and Cultural Rights (ICESCR) on 28 December 1978. The Covenant entered into force for New Zealand on 28 March 1979. Ratification means that Aotearoa New Zealand has formally agreed to be bound by the treaty in international law and is expected to take steps to implement and uphold its obligations in good faith, even where the rights have not been fully incorporated into domestic legislation. See International Covenant on Economic, Social and Cultural Rights, adopted 16 December 1966, UN General Assembly Resolution 2200A (XXI), <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights>; also see Vienna Convention on the Law of Treaties, opened for signature 23 May 1969, arts 26–27, https://legal.un.org/ilc/texts/instruments/english/conventions/1_1_1969.pdf.
- ¹⁰⁶ Virginia Dignum et al., “Background Paper: Human Rights and Artificial Intelligence,” see note 49 above.
- ¹⁰⁷ Demis Hassabis, “AlphaFold Reveals the Structure of the Protein Universe,” Google DeepMind, July 28, 2022, <https://deepmind.google/discover/blog/alphafold-reveals-the-structure-of-the-protein-universe/>; “Press Release: The Nobel Prize in Chemistry 2024,” Royal Swedish Academy of Sciences, October 9, 2024, <https://www.nobelprize.org/prizes/chemistry/2024/press-release/>. The 2024 Nobel Prize in Chemistry was awarded one half to David Baker for computational protein design and one half jointly to Demis Hassabis and John Jumper for protein-structure prediction; Hassabis and Jumper are the AlphaFold co-creators.

- ¹⁰⁸ SPRIND (Bundesagentur für Sprunginnovationen), “Sovereign Tech Fund — Strengthening Digital Sovereignty,” accessed July 23, 2026, <https://www.sprind.org/en/actions/projects/sovereign-tech-fund>; Sovereign Tech Agency, “Sovereign Tech Agency,” accessed July 23, 2026, <https://www.sovereign.tech>.
- ¹⁰⁹ Cybersecurity and Infrastructure Security Agency, “Apache Log4j Vulnerability Guidance,” last modified April 8, 2022, <https://www.cisa.gov/news-events/news/apache-log4j-vulnerability-guidance>.
- ¹¹⁰ For more on this right, see Office of the United Nations High Commissioner for Human Rights, “Freedom of Expression and Opinion,” <https://www.ohchr.org/en/topic/freedom-expression-and-opinion>; Office of the United Nations High Commissioner for Human Rights, “Special Rapporteur on the Promotion and Protection of the Right Freedom of Opinion and Expression,” <https://www.ohchr.org/en/special-procedures/sr-freedom-of-opinion-and-expression>; ARTICLE 19, “What Is Freedom of Expression?,” <https://www.article19.org/new-what-is-freedom-of-expression/>; see also “Freedom of Expression,” Max Planck Encyclopedia of Public International Law, Oxford Public International Law, <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e855>. For specific discussion of freedom of expression in relation to AI, see David Kaye, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/73/348 (2018), <https://docs.un.org/en/A/73/348>.
- ¹¹¹ Article 19(3) of the International Covenant on Civil and Political Rights: restrictions on the rights to freedom of expression and access to information must meet the standards of legality, meaning that they are publicly provided by a law that meets standards of clarity and precision and are interpreted by independent judicial authorities; necessity and proportionality, meaning that they are the least intrusive measure necessary to achieve the legitimate interest at hand and do not imperil the essence of the right; and legitimacy, meaning that they must be in pursuit of an enumerated legitimate interest, namely, the protection of rights or reputations of others, national security or public order, or public health or morals. David Kaye, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/73/348 (2018), para 28, <https://docs.un.org/en/A/73/348> (quoting Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/38/35 (2018), para 7).
- ¹¹² New Zealand Bill of Rights Act 1990 (NZ), s 14 “Freedom of Expression.” <https://www.legislation.govt.nz/act/public/1990/109/en/latest/#DLM224792>
- ¹¹³ *Yong Joo-Kang v. Republic of Korea*, Human Rights Committee Communication No. 878/1999, UN Doc CCPR/C/78/D/878/1999 (16 July 2003).
- ¹¹⁴ See RMIT Information Integrity Hub, “The Repost: December 2025,” RMIT University, December 5, 2025, <https://www.rmit.edu.au/about/schools-colleges/media-and-communication/industry/rmit-information-integrity-hub/the-repost/repost-december-2025>; Joint Declaration on Artificial Intelligence, Freedom of Expression and Media Freedom, adopted by the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression, and the ACHPR Special Rapporteur on Freedom of Expression and Access to Information in Africa (24 October 2025), <https://www.ohchr.org/sites/default/files/documents/issues/expression/statements/2025-10-24-joint-declaration-artificial-intelligence.pdf>.
- ¹¹⁵ David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/73/348 (2018), para 10, <https://docs.un.org/en/A/73/348>.

- ¹¹⁶ See Rachel George and Ian Klaus, “AI and Democracy: Mapping the Intersections,” Carnegie Endowment for International Peace, January 8, 2026, <https://carnegieendowment.org/research/2026/01/ai-and-democracy-mapping-the-intersections?lang=en>; OECD, “AI in Civic Participation and Open Government,” in *Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions* (Paris: OECD Publishing, 2025), https://www.oecd.org/en/publications/2025/06/governing-with-artificial-intelligence_398fa287/full-report/ai-in-civic-participation-and-open-government_51227ce7.html; and Lindsey Andersen, *Human Rights in the Age of Artificial Intelligence* (Access Now, 2018), 25, <https://www.accessnow.org/wp-content/uploads/2018/11/AI-and-Human-Rights.pdf>.
- ¹¹⁷ Meta’s Oversight Board — an independent body that reviews contested content-moderation decisions on Facebook and Instagram — explicitly grounds its rulings in international human rights law; see, for example, Oversight Board, “Protest Footage Paired With Pro-Duterte Chants,” November 25, 2025, <https://www.oversightboard.com/decision/fb-v6y3g1dv/>.
- ¹¹⁸ Abhilash Nandy et al., “YesBut: A High-Quality Annotated Multimodal Dataset for Evaluating Satire Comprehension Capability of Vision-Language Models,” in *Proceedings of the 2024 Conference on Empirical Methods in Natural Language Processing*, 16878–16895 (2024), <https://arxiv.org/pdf/2409.13592>.
- ¹¹⁹ For more information on this right, see United Nations and the Rule of Law, “Equality and Non-discrimination,” last modified February 19, 2019, <https://www.un.org/ruleoflaw/thematic-areas/human-rights/equality-and-non-discrimination/>; International Covenant on Civil and Political Rights, arts 2(1) and 26; and International Covenant on Economic, Social and Cultural Rights, art 2(2).
- ¹²⁰ See New Zealand Bill of Rights Act 1990 (NZ), see note 112 above s 19.
- ¹²¹ Human Rights Act 1993 (NZ), pt 2 (Prohibited Grounds of Discrimination), <https://www.legislation.govt.nz/act/public/1993/82/en/latest/#DLM304212>.
- ¹²² Royal Commission into the Robodebt Scheme (Commissioner Catherine Holmes AC SC), Report of the Royal Commission into the Robodebt Scheme (Canberra: Commonwealth of Australia, 2023), <https://robodebt.royalcommission.gov.au/publications/report>.
- ¹²³ Services Australia, “New Robodebt Class Action Settlement,” Australian Government, <https://www.servicesaustralia.gov.au/new-robodebt-class-action-settlement>.
- ¹²⁴ OECD, *Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions* (Paris: OECD Publishing, 2025), Box 5.6, <https://doi.org/10.1787/795de142-en>.
- ¹²⁵ Melissa Heikkilä, “Dutch Scandal Serves as a Warning for Europe over Risks of Using Algorithms,” *POLITICO*, March 29, 2022, <https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/>.
- ¹²⁶ Amnesty International, *Xenophobic Machines: Discrimination through Unregulated Use of Algorithms in the Dutch Childcare Benefits Scandal* (London: Amnesty International, 2021), EUR 35/4686/2021, <https://www.amnesty.org/en/documents/eur35/4686/2021/en/>.
- ¹²⁷ For more information on this right, see Office of the United Nations High Commissioner for Human Rights (OHCHR) and World Health Organization (WHO), *The Right to Health*, Fact Sheet No. 31, <https://www.ohchr.org/sites/default/files/Documents/Publications/Factsheet31.pdf>; and Committee on Economic, Social and Cultural Rights, General Comment No. 14 (2000), *The Right to the Highest Attainable Standard of Health*.
- ¹²⁸ Ibid.
- ¹²⁹ Ibid.
- ¹³⁰ A widely deployed US health algorithm systematically underestimated the health needs of Black patients because it used historical healthcare costs as a proxy for health need, and Black patients had historically received less care for the same level of illness. See Ziad Obermeyer et al., “Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations,” *Science* 366, no. 6464 (2019): 447–453, <https://doi.org/10.1126/science.aax2342>.

- ¹³¹ Office of the Privacy Commissioner, “Privacy Commissioner Finds Manage My Health and Health NZ Breached Privacy Act,” May 27, 2026, <https://www.privacy.org.nz/tuhono-connect/statements-media-releases/privacy-commissioner-finds-manage-my-health-and-health-nz-breached-privacy-act/>.
- ¹³² Hamilton Morrin et al., “Delusions by Design? How Everyday AIs Might Be Fuelling Psychosis (and What Can Be Done about It),” PsyArXiv (2025), https://doi.org/10.31234/osf.io/cmy7n_v5.
- ¹³³ Jasmine Ong et al., “Artificial Intelligence, ChatGPT, and Other Large Language Models for Social Determinants of Health,” *Cell Reports Medicine* (2024), [https://www.cell.com/cell-reports-medicine/fulltext/S2666-3791\(23\)00573-6](https://www.cell.com/cell-reports-medicine/fulltext/S2666-3791(23)00573-6); Rumi Chunara et al., “Social Determinants of Health: The Need for Data Science Methods and Capacity,” *Lancet Digital Health* (2024), [https://www.thelancet.com/journals/landig/article/PIIS2589-7500\(24\)00022-0/fulltext](https://www.thelancet.com/journals/landig/article/PIIS2589-7500(24)00022-0/fulltext); Mass General Brigham, “Generative AI Models Effectively Highlight Social Determinants of Health in Doctors’ Notes,” 2024, <https://www.massgeneralbrigham.org/en/about/newsroom/articles/generative-artificial-intelligence-models-effectively-highlight-social-determinants-of-health-in-doctors-notes>; Morelli, “Artificial Intelligence and Social Determinants of Health,” *Primary Care Clinics* (2025), [https://www.primarycare.theclinics.com/article/S0095-4543\(25\)00064-8/fulltext](https://www.primarycare.theclinics.com/article/S0095-4543(25)00064-8/fulltext); UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (Paris: UNESCO, 2021).
- ¹³⁴ UNESCO, “Right to Education,” UNESCO, accessed March 16, 2026, <https://www.unesco.org/en/right-education>. (The original footnote also cited the OHCHR Special Rapporteur on the right to education’s ‘about-right-education-and-human-rights’ page and the UNESCO document at unesdoc.unesco.org/ark:/48223/pf0000395373; neither is held as a converted file in-vault and their content could not be independently verified, so no citation is given for them here.)
- ¹³⁵ Committee on Economic, Social and Cultural Rights, *General Comment No. 13: The Right to Education (Article 13 of the Covenant)*, Twenty-First Session, UN Doc. E/C.12/1999/10 (8 December 1999)
- ¹³⁶ UNESCO, “What You Need to Know about AI and the Right to Education,” UNESCO, September 25, 2025, <https://www.unesco.org/en/articles/what-you-need-know-about-ai-and-right-education>.
- ¹³⁷ Ako Aotearoa, “Positive Uses of AI in Learning and Teaching,” Artificial Intelligence (AI) in Tertiary Education, accessed July 14, 2026, <https://ako.ac.nz/programmes-and-services/collections/artificial-intelligence-ai-in-tertiary-education/key-ideas/positive-uses-of-ai-in-learning-and-teaching>. But see also Nataliya Kosmyna et al., “Your Brain on ChatGPT: Accumulation of Cognitive Debt When Using an AI Assistant for Essay Writing Task,” arXiv preprint arXiv:2506.08872 (2025), <https://arxiv.org/abs/2506.08872>.
- ¹³⁸ For a full list of international instruments related to the right to education, see Office of the United Nations High Commissioner for Human Rights, “The Right to Human Rights Education: A Compilation of Provisions of International and Regional Instruments Dealing with Human Rights Education,” September 2014, <https://www.ohchr.org/en/resources/educators/human-rights-education-training/right-human-rights-education>.
- ¹³⁹ Te Kāhui Tika Tangata Human Rights Commission, “Tika ki te Whai Mahi — Right to Work,” Human Rights in Aotearoa, accessed July 14, 2026, <https://tikatangata.org.nz/human-rights-in-aotearoa/right-to-work>.
- ¹⁴⁰ See Committee on Economic, Social and Cultural Rights, *General Comment No. 18: The Right to Work (Art. 6 of the Covenant)*, UN Doc E/C.12/GC/18 (February 6, 2006), <https://www.refworld.org/legal/general/cescr/2006/32433>.
- ¹⁴¹ See Employment Relations Act 2000 (NZ), which protects workers’ rights in employment relationships, including good faith obligations, collective bargaining, freedom of association, and protection against unjustified dismissal and disadvantage; Health and Safety at Work Act 2015 (NZ), which protects workers’ health and safety in the workplace; and Minimum Wage Act 1983 (NZ) and Holidays Act 2003 (NZ); see also Human Rights Act 1993 (NZ).
- ¹⁴² UN General Assembly, *International Covenant on Economic, Social and Cultural Rights*, 993 UNTS 3, art 11 (adopted 16 December 1966, entered into force 3 January 1976).

- ¹⁴³ International Labour Organization, “AI-Driven Intrusive Surveillance and Loss of Autonomy at Work Linked to Psychosocial Risks for Employees,” ILO News, April 30, 2026, <https://www.ilo.org/resource/news/ai-driven-intrusive-surveillance-and-loss-autonomy-work-linked-psychosocial>.
- ¹⁴⁴ UN Development Programme, United Nations Environment Programme, and Office of the High Commissioner for Human Rights, What Is the Right to a Healthy Environment? (Information Note, January 2023), <https://www.undp.org/sites/g/files/zskgke326/files/2023-01/UNDP-UNEP-UNHCHR-What-is-the-Right-to-a-Healthy-Environment.pdf>.
- ¹⁴⁵ UN General Assembly, Resolution 76/300, “The Human Right to a Clean, Healthy and Sustainable Environment,” UN Doc A/RES/76/300 (28 July 2022); see also United Nations Human Rights Council, Resolution 48/13, “The Human Right to a Clean, Healthy and Sustainable Environment” (8 October 2021).
- ¹⁴⁶ UN Development Programme (UNDP), United Nations Environment Programme (UNEP), and Office of the United Nations High Commissioner for Human Rights (OHCHR), *What Is the Right to a Healthy Environment?*, Information Note (January 2023), <https://www.undp.org/sites/g/files/zskgke326/files/2023-01/UNDP-UNEP-UNHCHR-What-is-the-Right-to-a-Healthy-Environment.pdf>.
- ¹⁴⁷ Ibid.
- ¹⁴⁸ Ibid.
- ¹⁴⁹ Aotearoa New Zealand voted in favour of recognition of the right at the UN General Assembly. See UN General Assembly. Voting record for Resolution 76/300, *The Human Right to a Clean, Healthy and Sustainable Environment*. July 28, 2022. UN Digital Library, <https://digitallibrary.un.org/record/3982659>. UN General Assembly resolutions are not legally binding. However, they may carry significant normative and political weight, contribute to the development of international law, and provide evidence of emerging international human rights standards.
- ¹⁵⁰ According to the UN Environment Programme, “despite the lack of scientific evidence concerning water consumption of AI, it is estimated that the global demand for water resulting from AI may reach 4.2–6.6 billion cubic metres in 2027. Semiconductor production requires large amounts of pure water, while data centres use water indirectly or electricity generation and directly for cooling. The growing demand for data centres in warmer water scarce regions adds to water management challenges, leading to increased tension over water use between data centres and human need.” See UN Environment Programme, *Artificial Intelligence (AI) End-to-End: The Environmental Impact of the Full AI Life Cycle Needs to Be Comprehensively Assessed*, Issues Note (Nairobi: UNEP, September 21, 2024), para. 11, <https://wedocs.unep.org/rest/api/core/bitstreams/07b3c8fc-bd30-4b92-b5f4-d665e927b59d/content>.
- ¹⁵¹ UN Environment Programme, “AI Has an Environmental Problem. Here’s What the World Can Do About That,” *UNEP News and Stories*, September 21, 2024, updated November 13, 2025, <https://www.unep.org/news-and-stories/story/ai-has-environmental-problem-heres-what-world-can-do-about>; see also UN Environment Programme, *Artificial Intelligence (AI) End-to-End: The Environmental Impact of the Full AI Life Cycle Needs to Be Comprehensively Assessed*, Issues Note (Nairobi: UNEP, September 21, 2024), <https://wedocs.unep.org/items/5f3afe87-5419-439b-a6ee-14240b2605e9>.
- ¹⁵² See UN News, “AI’s Environmental Costs Threaten Water, Land and Climate,” June 4, 2026, <https://news.un.org/en/story/2026/06/1167658>.
- ¹⁵³ For more on this right, see UN General Assembly, *Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law*, GA Res. 60/147 (December 16, 2005), <https://www.ohchr.org/en/instruments-mechanisms/instruments/basic-principles-and-guidelines-right-remedy-and-reparation>; International Commission of Jurists et al., “Background Information Concerning the Right to Remedy and Reparation,” ICJ, 2002, <https://www.icj.org/resource/background-information-concerning-the-right-to-remedy-and-reparation/>.
- ¹⁵⁴ OHCHR, *The Right to Privacy in the Digital Age*, see note 53 above.

- ¹⁵⁵ Human Rights Committee, General Comment No. 31 (2004): The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, UN Doc CCPR/C/21/Rev.1/Add.13, para 15.
- ¹⁵⁶ *Simpson v Attorney-General (Baigent's Case)* [1994] 3 NZLR 667 (CA).
- ¹⁵⁷ This idea originates from the European Court of Human Rights; see Department for the Execution of Judgments of the European Court of Human Rights, Council of Europe, *Excessive Formalism by Courts*: Thematic Factsheet, accessed July 14, 2026, <https://rm.coe.int/thematic-factsheet-excessive-formalism-courts-eng-docx/1680aae7f4>; but is used to inform understanding of the right to remedy under international law more generally, see OHCHR, "Access to Remedy," Working Group on Business and Human Rights, accessed July 14, 2026, <https://www.ohchr.org/en/special-procedures/wg-business/access-remedy>.
- ¹⁵⁸ See Center for Democracy and Technology (CDT) Europe, "Effective Remedies in AI: An Insufficiently Explored Avenue for AI Accountability," CDT, accessed July 14, 2026, <https://cdt.org/insights/effective-remedies-in-ai-an-insufficiently-explored-avenue-for-ai-accountability/>.
- ¹⁵⁹ OECD.AI, "AI in Government: Issues > Justice," OECD AI Policy Observatory, accessed July 14, 2026, <https://oecd.ai/en/gov/issues/justice>.
- ¹⁶⁰ Keoni Mahelona, Gianna Leoni, Suzanne Duncan, and Miles Thompson. 2023. "OpenAI's Whisper Is Another Case Study in Colonisation." *Papa Reo (blog)*, *Te Hiku Media*. <https://blog.papareo.nz/whisper-is-another-case-study-in-colonisation/>.
- ¹⁶¹ UN General Assembly, *Convention on the Rights of the Child*, adopted November 20, 1989, *United Nations Treaty Series*, vol. 1577, p. 3, entered into force September 2, 1990.
- ¹⁶² See Committee on the Rights of the Child, General Comment No. 14 (2013) on the Right of the Child to Have His or Her Best Interests Taken as a Primary Consideration (Art. 3, para. 1), UN Doc. CRC/C/GC/14 (29 May 2013) and Committee on the Rights of the Child, General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, UN Doc. CRC/C/GC/25 (2 March 2021).
- ¹⁶³ Committee on the Rights of the Child, General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, UN Doc. CRC/C/GC/25 (2 March 2021).
- ¹⁶⁴ UN General Assembly, *Convention on the Rights of Persons with Disabilities*, adopted December 13, 2006, *UNTS* vol. 2515, p. 3, entered into force May 3, 2008.
- ¹⁶⁵ Margaret Yun-Pu Tu, "AI Threatens Indigenous Data Sovereignty and Digital Self-Determination," *Policy Options* (Institute for Research on Public Policy), May 22, 2025, <https://policyoptions.irpp.org/2025/05/ai-indigenous-data/>; see also OHCHR, "Indigenous Sovereignty in the AI Era," August 2025, <https://www.ohchr.org/en/stories/2025/08/indigenous-sovereignty-ai-era>.
- ¹⁶⁶ United Nations Declaration on the Rights of Indigenous Peoples, GA Res 61/295, UN Doc A/RES/61/295 (13 September 2007); and Expert Mechanism on the Rights of Indigenous Peoples, "Right of Indigenous Peoples to Data, Including with Regard to Data Collection and Disaggregation," UN Doc A/HRC/60/66 (2025), Expert Mechanism Advice No. 18 (2025) annex, paras 20–22, <https://www.ohchr.org/en/documents/thematic-reports/ahrc6066-right-indigenous-peoples-data-including-regard-data-collection>.
- ¹⁶⁷ Te Taka Keegan, personal communication, June 26, 2026.
- ¹⁶⁸ Kate Vredenburg, "The Right to Explanation," *Journal of Political Philosophy* 30, no. 2 (2022): 209–229, <https://doi.org/10.1111/jopp.12262>; Yuval Shany, "From Digital Rights to International Human Rights: The Emerging Right to a Human Decision Maker," *AI Ethics at Oxford Blog* (blog), December 11, 2023, <https://www.oxford-aiethics.ox.ac.uk/blog/digital-rights-international-human-rights-emerging-right-human-decision-maker>; Peter Douglas, "Understanding Right to Explanation and Automated Decision-Making in Europe's GDPR and AI Act," *Tech Policy Press*, September 19, 2025, <https://www.techpolicy.press/understanding-right-to-explanation-and-automated-decisionmaking-in-europes-gdpr-and-ai-act/>.

- ¹⁶⁹ European Union, Regulation (EU) 2024/1689 of the European Parliament and of the Council (Artificial Intelligence Act), art 86, <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>; European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), arts 13–15, <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.
- ¹⁷⁰ GDPR art 22 provides for “the right not to be subject to a decision based solely on automated processing,” known as ‘human in the loop’: European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), art 22, <https://eur-lex.europa.eu/eli/reg/2016/679/oj>. See also the discussion of potential new and emerging rights in Yuval Shany, *The Need for and Feasibility of an International AI Bill of Human Rights* (Accelerator Fellowship Programme, Institute for Ethics in AI, University of Oxford, November 2025), <https://afp.oxford-aiethics.ox.ac.uk/sitefiles/white-paper-professor-yuval-shany.pdf>.
- ¹⁷¹ International Covenant on Civil and Political Rights, opened for signature 16 December 1966 (UN General Assembly resolution 2200A (XXI)), art 19.
- ¹⁷² Office of the United Nations High Commissioner for Human Rights, *Mapping Report: Human Rights and New and Emerging Digital Technologies*, UN Doc A/HRC/56/45 (20 August 2024), para 4 (“The Internet is an indispensable enabler of human rights.”).
- ¹⁷³ International Covenant on Civil and Political Rights, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976), art 17.
- ¹⁷⁴ David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN Doc A/73/348 (29 August 2018), para 22, recalling his earlier report *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN Doc A/HRC/29/32 (2015).
- ¹⁷⁵ Pascal Lupien, “Indigenous Movements, Collective Action, and Social Media: New Opportunities or New Threats?” *Social Media + Society* 6, no. 2 (2020): 1–11, <https://doi.org/10.1177/2056305120926487>; Jin Young Hwang, “Social Media’s Impact on Community Building and Social Movements,” *Magna Scientia Advanced Research and Reviews* 13, no. 2 (2025): 175–87, <https://doi.org/10.30574/msarr.2025.13.2.0056>.
- ¹⁷⁶ Cole Stryker, “What Is Multimodal AI?,” IBM Think, July 15, 2024, <https://www.ibm.com/think/topics/multimodal-ai>.
- ¹⁷⁷ Tim Young, personal communication, April 13, 2026.
- ¹⁷⁸ Te Hiku Media, “Enabling a Sovereign Digital Future for Indigenous Languages,” Papa Reo, accessed March 15, 2026, <https://papareo.nz/#kaupapa>.
- ¹⁷⁹ Peter-Lucas Jones, personal communication, May 20, 2026.
- ¹⁸⁰ Te Hiku Media, “Enabling a Sovereign Digital Future for Indigenous Languages,” Papa Reo, accessed March 15, 2026, <https://papareo.nz/>.
- ¹⁸¹ Ibid.
- ¹⁸² Te Hiku Media, “Kaituhi — Automatic Te Reo Māori, NZ English and Bilingual Transcriptions,” Kaituhi, accessed March 15, 2026, <https://kaituhi.nz/>.
- ¹⁸³ Te Hiku Media, “Enabling a Sovereign Digital Future for Indigenous Languages,” Papa Reo, accessed March 15, 2026, <https://papareo.nz/>; see also Te Hiku Media, “Kaitiakitanga License,” GitHub, <https://github.com/TeHikuMedia/Kaitiakitanga-License>.
- ¹⁸⁴ Hamish Fraser and Tom Barraclough, “Governing Digital Legal Systems: Insights on Artificial Intelligence and Rules as Code.” MIT Computational Law Report. (2024). <https://law.mit.edu/pub/governingdigitallegalsystems>.
- ¹⁸⁵ Yun Sin Koh, personal communication, July 8, 2026.
- ¹⁸⁶ UN Committee on Economic, Social and Cultural Rights, General Comment No. 25 (2020) see note 100 above, paras 16, 47.

- ¹⁸⁷ United Nations Office of the High Commissioner for Human Rights, Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework, HR/PUB/11/04 (New York and Geneva: United Nations, 2011), 1–3, <https://www.ohchr.org/en/publications/reference-publications/guiding-principles-business-and-human-rights>; UN Working Group on Business and Human Rights, “Procurement and Deployment of Artificial Intelligence Must Be Aligned with Human Rights: UN Experts,” Press Release, June 26, 2025; Council of Europe, Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, opened for signature September 5, 2024, preamble.
- ¹⁸⁸ The term itself became institutionalised through the UN’s human rights-based approach: United Nations Development Group, The Human Rights Based Approach to Development Cooperation: Towards a Common Understanding among UN Agencies (2003). <https://unsdg.un.org/resources/human-rights-based-approach-development-cooperation-towards-common-understanding-among-un>.
- ¹⁸⁹ See UN Guiding Principles on Business and Human Rights, John Ruggie, Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises: Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework, UN Doc. A/HRC/17/31 (March 21, 2011).
- ¹⁹⁰ For example, obligations under the Charter of the United Nations: under the Charter, all UN member states accept a set of binding international legal obligations, including important commitments related to human rights. While the Charter does not list detailed rights the way later treaties do, it establishes foundational duties including international cooperation, non-discrimination, and promoting universal respect for human rights and fundamental freedoms see, e.g., Charter of the United Nations, preamble, art 1(3), arts 55–56, opened for signature June 26, 1945, <https://www.un.org/en/about-us/un-charter/full-text>.
- ¹⁹¹ This is an accepted typology which originates from legal scholarship of Henry Shue, Basic Rights: Subsistence, Affluence, and U.S. Foreign Policy (Princeton, NJ: Princeton University Press), and Asbjørn Eide, <https://digitallibrary.un.org/record/139080?ln=en&v=pdf>, and is entrenched in treaty interpretations — for example, the UN Office of the High Commissioner for Human Rights explicitly aligns these obligations with international human rights treaties. See UN Committee on Economic, Social and Cultural Rights, “State Obligations in the Context of Business Activities,” General Comment No. 24, E/C.12/GC/24, <https://docs.un.org/en/E/C.12/GC/24>; and United Nations Office of the High Commissioner for Human Rights, Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework, HR/PUB/11/04 (New York and Geneva: United Nations, 2011), https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinessshr_en.pdf. For more on this related to AI and new technologies, see United Nations Office of the High Commissioner for Human Rights, Human Rights and Technical Standard-Setting Processes for New and Emerging Digital Technologies: Report of the Office of the United Nations High Commissioner for Human Rights (Human Rights Council, fifty-third session, 2023), <https://digitallibrary.un.org/record/4031373?v=pdf&ln=en>.
- ¹⁹² A human-rights approach to AI governance requires not only protection from AI-related harms, but also respect for individuals’ freedom to access and use AI tools. Consistent with Article 19 of the ICCPR, limitations on AI use should be justified, necessary and proportionate. Where the use of AI does not interfere with the rights and freedoms of others, individuals should enjoy a presumptive freedom to use such technologies for expression, information-seeking, learning, creativity, research and innovation. See UN Human Rights Committee, General Comment No. 34: Article 19 (Freedoms of Opinion and Expression); International Covenant on Civil and Political Rights, opened for signature 16 December 1966, entered into force 23 March 1976, art 19.
- ¹⁹³ *Yorston v Attorney-General* [2026] NZCA 15 (Court of Appeal of New Zealand, February 10, 2026).
- ¹⁹⁴ For more information on progressive realisation see Committee on Economic, Social and Cultural Rights, General Comment No. 3: The Nature of States Parties’ Obligations (Article 2, Paragraph 1), UN Doc E/1991/23 (1990); Haris Huremagić, “Core Obligations and Progressive Realization,” in Elgar Encyclopedia of Human Rights (Edward Elgar Publishing, 2022), 371–377, <https://>

doi.org/10.4337/9781789903621.core.obligations.progressive.realization; Ben Saul, David Kinley, and Jacqueline Mowbray, “Article 2(1): Progressive Realization of ICESCR Rights,” in *The International Covenant on Economic, Social and Cultural Rights: Commentary, Cases, and Materials* (Oxford Academic, 2014), <https://doi.org/10.1093/law/9780199640300.003.0003>.

¹⁹⁵ See Committee on Economic, Social and Cultural Rights, General Comment No. 13: The Right to Education (Article 13), UN Doc E/C.12/1999/10 (1999).

¹⁹⁶ See Committee on Economic, Social and Cultural Rights, General Comment No. 25 (2020) note 100 above.

¹⁹⁷ UN Human Rights Council, New and Emerging Digital Technologies and Human Rights, Resolution A/HRC/RES/59/11 (adopted 7 July 2025).

¹⁹⁸ UN Human Rights Council. 2025. *Artificial Intelligence Procurement and Deployment: Ensuring Alignment with the Guiding Principles on Business and Human Rights; Report of the Working Group on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises*. A/HRC/59/53. Geneva: United Nations. <https://www.ohchr.org/en/documents/thematic-reports/ahrc5953-artificial-intelligence-procurement-and-deployment-ensuring>.

¹⁹⁹ Servet Yanatma, “Nvidia Surpasses Germany: How the Market Caps of Tech Giants Compare to Top Economies,” *Euronews*, May 16, 2026, <https://www.euronews.com/business/2026/05/16/nvidia-surpasses-germany-how-the-market-caps-of-tech-giants-compare-to-top-economies>.

²⁰⁰ See UN Trade and Development (UNCTAD), “Highly Concentrated Digital Markets Put Consumers at Risk. Here’s How to Change Course,” UNCTAD News, July 8, 2025, <https://unctad.org/news/highly-concentrated-digital-markets-put-consumers-risk-heres-how-change-course>.

²⁰¹ UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, SHS/BIO/PI/2021/1 (Paris: UNESCO, 2021), <https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence>.

²⁰² Working Group on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, *Artificial Intelligence Procurement and Deployment: Ensuring Alignment with the Guiding Principles on Business and Human Rights*, UN Doc. A/HRC/59/53 (14 May 2025).

²⁰³ United Nations Office of the High Commissioner for Human Rights, *Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework* (Geneva and New York: United Nations, 2011), https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinessshr_en.pdf.

²⁰⁴ Natalie Stadelmann and Isabel Ebert, *AI and Human Rights 101*, Human Rights and AI Series (UN Global Compact Academy and OHCHR B-Tech Project, 2025), <https://www.ohchr.org/sites/default/files/2025-10/ai-series-1-en.pdf>; also see Office of the United Nations High Commissioner for Human Rights, “Procurement and Deployment of Artificial Intelligence Must Be Aligned with Human Rights: UN Experts,” OHCHR Press Releases, June 2025, <https://www.ohchr.org/en/press-releases/2025/06/procurement-and-deployment-artificial-intelligence-must-be-aligned-human>.

²⁰⁵ Natalie Stadelmann and Isabel Ebert, *AI and Human Rights 101*, Human Rights and AI Series (UN Global Compact Academy and OHCHR B-Tech Project, 2025), <https://www.ohchr.org/sites/default/files/2025-10/ai-series-1-en.pdf>.

²⁰⁶ OECD, *OECD Guidelines for Multinational Enterprises on Responsible Business Conduct* (Paris: OECD Publishing, 2023), <https://doi.org/10.1787/81f92357-en>.

²⁰⁷ OECD, *OECD Due Diligence Guidance for Responsible AI* (OECD Publishing, Paris, 2026), <https://doi.org/10.1787/41671712-en>.

²⁰⁸ European Union, Regulation (EU) 2024/1689 of the European Parliament and of the Council (Artificial Intelligence Act), art 3(56), <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>.

- ²⁰⁹ European Parliament and Council of the European Union, *Directive (EU) 2024/1760 of 13 June 2024 on Corporate Sustainability Due Diligence and Amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859*, OJ L 2024/1760 (5 July 2024).
- ²¹⁰ European Parliament and Council of the European Union, Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), OJ L 277 (27 October 2022): 1–102 <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act>
- ²¹¹ Office of the United Nations High Commissioner for Human Rights (OHCHR), *Practical Application of the Guiding Principles on Business and Human Rights to the Activities of Technology Companies, Including Activities Relating to Artificial Intelligence* (advance edited version), UN Doc A/HRC/59/32 (2025), <https://www.ohchr.org/en/documents/thematic-reports/ahrc5932-practical-application-guiding-principles-business-and-human>.
- ²¹² UNDRIP see note 46 above Arts 1, 40.
- ²¹³ UNICEF, definition of “Rights Holders,” in United Nations Economic and Social Commission for Western Asia, *Sustainable Development Glossary*, accessed July 14, 2026, <https://www.unescwa.org/sd-glossary/rights-holders>.
- ²¹⁴ Te Mana Raraunga *Principles of Māori Data Sovereignty*, see note 77 above.
- ²¹⁵ Te Kāhui Raraunga, *Māori AI Governance: A Framework for Ethical Governance of AI in Aotearoa* see note 25 above.
- ²¹⁶ Civil Aviation Authority of New Zealand, “Civil Aviation Rules,” aviation.govt.nz, accessed July 23, 2026, <https://www.aviation.govt.nz/rules/rule-part/>; Civil Aviation Act 2023 (NZ), <https://www.legislation.govt.nz/act/public/2023/10/en/>
- ²¹⁷ Ibid.
- ²¹⁸ Ibid.
- ²¹⁹ Ibid.
- ²²⁰ Ibid.
- ²²¹ Ibid.
- ²²² McKinsey & Company, “What is sovereign AI” (March 2026), <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-sovereign-ai>
- ²²³ Stanford HAI, “AI Sovereignty’s Definitional Dilemma” (February 2026), <https://hai.stanford.edu/news/ai-sovereigntys-definitional-dilemma>.
- ²²⁴ Te Hiku Media, “Kaitiakitanga License,” GitHub, <https://github.com/TeHikuMedia/Kaitiakitanga-License>.
- ²²⁵ Tech Policy Design Institute *From AI Sovereignty to AI Agency* (2025), <https://techpolicy.au/wp-content/uploads/2025/11/TPDi-AI-Agency-Discussion-Paper-November-2025-1.pdf>.
- ²²⁶ The Public AI Network, *Public AI: Infrastructure for the Common Good* (2024), <https://publicknowledge.org/policy/public-ai-infrastructure-for-the-common-good-white-paper/>.
- ²²⁷ Committee on Economic, Social and Cultural Rights, General Comment No. 25 See note 100 above.
- ²²⁸ On the US CLOUD Act, see Clarifying Lawful Overseas Use of Data Act, Pub. L. No. 115-141, div. V, 132 Stat. 1213 (2018); on the CJEU’s Schrems decisions, see Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650 (CJEU, Grand Chamber, 6 October 2015) (“Schrems I”); and Case C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, ECLI:EU:C:2020:559 (CJEU, Grand Chamber, 16 July, 2020) (“Schrems II”).
- ²²⁹ Richard Boast, “Te Tango Whenua — Māori Land Alienation,” *Te Ara: The Encyclopedia of New Zealand* (Ministry for Culture and Heritage Te Manatū Taonga), accessed July 14, 2026, <https://teara.govt.nz/en/te-tango-whenua-maori-land-alienation/print>; Cathy Marr, *Public Works Takings of Maori Land, 1840–1981* (Rangahaua Whanui Series, National Theme G, prepared

for the Treaty of Waitangi Policy Unit, 1994; Wellington: Waitangi Tribunal, 1997), <https://www.waitangitribunal.govt.nz/assets/Rangahaua-whanui/THEME/Theme-G-Marr-Public-Works.pdf>.

²³⁰ Te Mana Raraunga, *Principles of Māori Data Sovereignty* see note 77 above.

²³¹ Tahu Kukutai et al., *Māori Data Governance Model*, see note 76 above.

²³² Te Kāhui Raraunga, *Māori AI Governance: A Framework for Ethical Governance of AI in Aotearoa* see note 25 above.

²³³ Te Hiku Media, “Papa Reo — Enabling a Sovereign Digital Future for Indigenous Languages,” Papa Reo, accessed March 15, 2026, <https://papareo.nz/>; Te Hiku Media, “Kaituhi — Automatic Te Reo Māori, NZ English, and Bilingual Transcriptions,” Kaituhi, accessed March 15, 2026, <https://kaituhi.nz/>.

²³⁴ Stats NZ, “Co-designing Māori Data Governance,” Data.govt.nz, last reviewed February 2, 2021, <https://data.govt.nz/toolkit/data-governance/maori>.

²³⁵ AI Forum New Zealand, *AI Blueprint for Aotearoa: A Refreshed Vision to 2030* (May 2026), <https://aiforum.org.nz/2026/05/06/ai-blueprint-for-aotearoa-a-refreshed-vision-to-2030/>.

²³⁶ New Zealand Government, Digitising Government Programme (Government Chief Digital Officer), “Digital Target State,” Digital.govt.nz, <https://dns.govt.nz/digital-government/digitising-government-programme-dgp/digital-target-state>.

²³⁷ Human Rights Act 1993 (NZ), s 5(2)(m), <https://legislation.govt.nz/act/public/1993/82/en/latest/#DLM304276>.

²³⁸ United Nations Committee on Economic, Social and Cultural Rights, General Comment No. 25 see note 100 above, para 76: “taking into account that many of the emerging inequalities are strongly linked to the capacity of some business entities to access, store and exploit massive data, it is crucial to regulate the ownership and control of data according to human rights principles.”

²³⁹ Risk assessment and impact assessment are related and overlapping tools. We have used ‘risk assessment’ as the main term throughout the rest of this section.

²⁴⁰ UN Development Programme, *Human Rights Impact of AI Assessment Toolkit* (2025), https://www.undp.org/sites/g/files/zskgke326/files/2025-12/undp_ai_hria_toolkit_final_publication_03.12.25_approved.pdf. See also Access Now’s 2022 *Human Rights Impact Assessments for AI: Analysis and Recommendations*. [Access Now Version — Human Rights Implications of Algorithmic Impact Assessments: Priority Recommendations to Guide Effective Development and Use](#) and Danish Institute for Human Rights & European Centre for Not-for-Profit Law’s 2025 *A Guide to Fundamental Rights Impact Assessments (“FRIA”) Under the EU Artificial Intelligence Act*. [ECNL DIHR Guide to FRIA Dec 2025.pdf](#)

²⁴¹ See Office of the United Nations High Commissioner for Human Rights (OHCHR), *Identifying and Assessing Human Rights Risks Related to End-Use: A B-Tech Foundational Paper* (Geneva: United Nations, 2021), <https://www.ohchr.org/Documents/Issues/Business/B-Tech/identifying-human-rights-risks.pdf> and Business & Human Rights Resource Centre, “Human Rights Due Diligence & Impact Assessment,” last modified March 12, 2025, <https://www.business-humanrights.org/en/big-issues/governing-business-human-rights/human-rights-due-diligence-impact-assessment>

²⁴² See Office of the United Nations High Commissioner for Human Rights (OHCHR), *Identifying and Assessing Human Rights Risks Related to End-Use: A B-Tech Foundational Paper* (Geneva: United Nations, 2021), <https://www.ohchr.org/Documents/Issues/Business/B-Tech/identifying-human-rights-risks.pdf>; Business & Human Rights Resource Centre, “Human Rights Due Diligence & Impact Assessment,” last modified March 12, 2025, <https://www.business-humanrights.org/en/big-issues/governing-business-human-rights/human-rights-due-diligence-impact-assessment/>; Business & Human Rights Resource Centre, “UNGPs Guidance & Implementation,” last modified October 21, 2024, <https://www.business-humanrights.org/en/big-issues/governing-business-human-rights/guidance-implementation>

- ²⁴³ For example the European Network of National Human Rights Institutions has highlighted such initiatives as emerging good practice for NHRIs working on AI and human rights see European Network of National Human Rights Institutions (ENNHRI), AI Resource: Putting Human Rights at the Heart of Artificial Intelligence (Brussels) <https://ennhri.org/ai-resource/>; UN, OECD and Council of Europe have all highlighted the key role of NHRI in overseeing, advising on, contributing to, and in some cases conducting such assessments as part of their mandate to protect and promote human rights
- ²⁴⁴ See National Human Rights Commission of Korea (NHRCK), Human Rights Impact Assessment Tool for AI (Seoul: NHRCK, 2024) <https://www.humanrights.go.kr/eng/board/read?boardManagementNo=7003&boardNo=7610408&menuLevel=2&menuNo=114>
- ²⁴⁵ See Danish Institute for Human Rights, A Guide to Fundamental Rights Impact Assessments under the EU Artificial Intelligence (AI) Act (Copenhagen: Danish Institute for Human Rights, December 15, 2025), <https://www.humanrights.dk/publications/guide-fundamental-rights-impact-assessments-under-eu-artificial-intelligence-ai-act>
- ²⁴⁶ See Equality and Human Rights Commission (Great Britain), Assessing the Equality Impact of AI-Based Technology: Six Discussion Points (Manchester: EHRC, March 24, 2025), <https://www.equalityhumanrights.com/guidance/assessing-equality-impact-ai-based-technology-six-discussion-points>
- ²⁴⁷ Stats NZ, “Algorithm Impact Assessment Toolkit,” data.govt.nz, <https://data.govt.nz/toolkit/data-ethics/government-algorithm-transparency-and-accountability/algorithm-impact-assessment-toolkit>.
- ²⁴⁸ New Zealand Ministry of Social Development, “Using Personal Information Responsibly: The Privacy, Human Rights and Ethics Framework,” msd.govt.nz, <https://www.msd.govt.nz/about-msd-and-our-work/work-programmes/initiatives/phrae/index.html>; and New Zealand Ministry of Social Development, “Automated Decision Making Standard,” mirrored via DocRef NZ AI Policy, <https://www.msd.govt.nz/about-msd-and-our-work/work-programmes/initiatives/phrae/adm-standard.html>.
- ²⁴⁹ Office of the Privacy Commissioner Te Mana Mātāpono Matatapu, *Biometric Processing Privacy Code 2025* (made under s 32 of the Privacy Act 2020 by the Privacy Commissioner, 21 July 2025), <https://www.privacy.org.nz/privacy-principles/codes-of-practice/biometric-processing-privacy-code/>.
- ²⁵⁰ Government Chief Digital Officer (New Zealand), “Responsible AI Guidance for the Public Service: GenAI,” Department of Internal Affairs, 2025, <https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/artificial-intelligence/responsible-ai-guidance-for-the-public-service-genai>.
- ²⁵¹ Royal Society Te Apārangi, *Guidelines for the Best-Practice Use of Generative Artificial Intelligence in Research in Aotearoa New Zealand* (June 2025), <https://www.royalsociety.org.nz/what-we-do/research-practice/generative-artificial-intelligence-in-research-in-aotearoa-new-zealand/guidelines-for-the-best-practice-use-of-generative-artificial-intelligence-in-research-in-aotearoa-new-zealand>.
- ²⁵² MBIE, *Responsible AI Guidance for Businesses* see note 20 above.
- ²⁵³ Digital Identity Services Trust Framework Regulations 2024 (NZ).
- ²⁵⁴ Te Kāhui Raraunga, *Māori AI Governance: A Framework for Ethical Governance of AI in Aotearoa* see note 25 above.
- ²⁵⁵ Human rights risk assessments have a long history of use as part of human rights due diligence. The Office of the United Nations High Commissioner for Human Rights’ mapping report records that human rights due diligence “is becoming a central element of efforts to respond to human rights challenges linked to digital technologies”: Office of the United Nations High Commissioner for Human Rights, *Mapping Human Rights and New and Emerging Digital Technologies*, UN Doc A/HRC/56/45 (2024), para 63. The Committee on Economic, Social and Cultural Rights notes that, in relation to the right to enjoy the benefits of scientific progress and its applications, states should establish a legal framework that imposes on non-state actors a duty of human rights due diligence, especially in the case of big technology companies (see A/74/493); this legal

framework should include measures that require companies to prevent discrimination at both the input and output levels of artificial intelligence systems and other technologies: Committee on Economic, Social and Cultural Rights, General Comment No. 25 n100 above, para 75.

- ²⁵⁶ See European Center for Not-for-Profit Law (ECNL) and Danish Institute for Human Rights (DIHR), “A Guide to Fundamental Rights Impact Assessments (‘FRIA’) Under the EU Artificial Intelligence Act” (December 2025), <https://ecnl.org/sites/default/files/2025-12/ECNL%20DIHR%20Guide%20to%20FRIA%20Dec%202025.pdf>; European Center for Not-for-Profit Law (ECNL) and Access Now, “Towards Meaningful Fundamental Rights Impact Assessments Under the DSA” (September 2023), <https://ecnl.org/sites/default/files/2023-09/Towards%20Meaningful%20FRIAs%20under%20the%20DSA%20Access%20Now.pdf>.
- ²⁵⁷ Regulation (EU) 2024/1689 of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), art 27 (Fundamental Rights Impact Assessment for High-Risk AI Systems), <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>.
- ²⁵⁸ OECD, *Due Diligence Guidance for Responsible AI* see 207
- ²⁵⁹ Council of Europe, Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, CETS No. 225, opened for signature 5 September 2024, Vilnius, <https://rm.coe.int/1680afae3c>.
- ²⁶⁰ Government of Canada, “Algorithmic Impact Assessment,” accessed July 23, 2026, <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html>.
- ²⁶¹ National Human Rights Commission of Korea, *Human Rights Impact Assessment Tool for AI* (Seoul: National Human Rights Commission of Korea, 2024), https://www.humanrights.go.kr/download/BASIC_ATTACH?storageNo=10005586.
- ²⁶² Digital NSW, “NSW AI Assessment Framework,” accessed July 23, 2026, <https://www.digital.nsw.gov.au/policy/artificial-intelligence/ai-governance-assurance-and-frameworks/nsw-ai-assessment-framework>
- ²⁶³ Te Kāhui Raraunga, *Māori AI Governance: A Framework for Ethical Governance of AI in Aotearoa* see note 25 above Tahu Kukutai et al., *Māori Data Governance Model*, see note 77 above.
- ²⁶⁴ New Zealand Ministry of Social Development, Automated Decision Making Standard (Ministry of Social Development, 2022), <https://www.msd.govt.nz/about-msd-and-our-work/work-programmes/initiatives/phrae/adm-standard.html>
- ²⁶⁵ Ministry of Social Development, “Using Personal Information Responsibly: The Privacy, Human Rights and Ethics (PHRaE) Framework,” MSD, accessed March 15, 2026, <https://www.msd.govt.nz/about-msd-and-our-work/work-programmes/initiatives/phrae/index.html>.
- ²⁶⁶ Te Kāhui Tika Tangata Human Rights Commission, *Privacy, Data and Technology: Human Rights Challenges in the Digital Age* (Auckland: New Zealand Human Rights Commission, 2018), <https://tikatangata.org.nz/our-work/privacy-data-and-technology-human-rights-challenges-in-the-digital-age>.
- ²⁶⁷ Office of the Privacy Commissioner, “Biometric Processing Privacy Code 2025,” accessed July 23, 2026, <https://www.privacy.org.nz/privacy-principles/codes-of-practice/biometric-processing-privacy-code/>.
- ²⁶⁸ New Zealand Government, Digital Public Service Branch, Department of Internal Affairs, “Trust Framework,” Digital.govt.nz, accessed July 23, 2026, <https://www.digital.govt.nz/standards-and-guidance/identity/trust-framework>.
- ²⁶⁹ *Digital Identity Services Trust Framework Act 2023* (NZ), 2023/13, <https://www.legislation.govt.nz/act/public/2023/13/en/latest/#LMS459583>
- ²⁷⁰ European Parliament and Council of the European Union, *Regulation (EU) 2024/1689 of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, OJ L 2024/1689 (12 July 2024), <http://data.europa.eu/eli/reg/2024/1689/oj>
- ²⁷¹ Ibid Article 3 (56)

- ²⁷² UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (Paris: UNESCO, 2021), para 101, <https://unesdoc.unesco.org/ark:/48223/pf0000381137>.
- ²⁷³ Ministry of Education Singapore, “Artificial Intelligence in Education,” last updated June 2, 2026, <https://www.moe.gov.sg/education-in-sg/educational-technology-journey/edtech-masterplan/artificial-intelligence-in-education>
- ²⁷⁴ Digital Equity Coalition Aotearoa (DECA), *A Fair Chance for All: Breaking the Cycle of Persistent Disadvantage* (submission to the New Zealand Productivity Commission, 11 November 2022), para 15, <https://www.treasury.govt.nz/sites/default/files/2024-05/pc-inq-fcfa-dr-136-digital-equity-coalition-aotearoa.pdf>.
- ²⁷⁵ Ibid.
- ²⁷⁶ New Zealand, Department of Internal Affairs (Te Tari Taiwhenua), *Long-Term Insights Briefing: How Can Community Participation and Decision-Making Be Better Enabled by Technology?* (Wellington: Department of Internal Affairs, November, 2022), ‘Option 1: Treating Access to Digital Technology as a Human Right and Meeting Aotearoa’s Digital Inclusion Goals.’
- ²⁷⁷ OECD, *Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions* (Paris: OECD Publishing, 2025), sec. “Procurement as a Lever for Public Good and Trustworthy AI,” <https://doi.org/10.1787/795de142-en>.
- ²⁷⁸ Government Chief Digital Officer, “Digital Investment and Procurement Principles,” NZ Digital Government, last modified February 23, 2026, <https://dns.govt.nz/digital-government/digitising-government-programme-dgp/digital-investment-and-procurement-principles>; New Zealand Government Procurement, “Government Procurement Rules: Responsible Expenditure of Public Funds,” 5th ed., [procurement.govt.nz](https://www.procurement.govt.nz), Ministry of Business, Innovation and Employment, accessed March 15, 2026, <https://www.procurement.govt.nz/government-procurement-framework/government-procurement-rules/>.
- ²⁷⁹ See for example Fibre Fale, “A Platform for Pacific People in Tech,” *Fibre Fale*, accessed July 14, 2026, <https://www.fibrefale.com/>.
- ²⁸⁰ Parliamentary Counsel Office, “Secondary Legislation Access Standards — Overview,” Making Secondary Legislation, accessed July 20, 2026, <https://www.pco.govt.nz/making-secondary-legislation/secondary-legislation-access-standards-intro>; Syncopate Lab, *R&D on Access to Legislation Data*, report prepared for the Parliamentary Counsel Office, New Zealand, June 28, 2024, <https://www.pco.govt.nz/about-us/legislative-data-and-technology/Report-on-access-to-legislation-data-from-syncopate-labs-2024>; New Zealand Government Chief Digital Officer, “Web Accessibility Standard 1.2,” Digital.govt.nz, Department of Internal Affairs, last modified March 10, 2025, <https://www.digital.govt.nz/standards-and-guidance/nz-government-web-standards/web-accessibility-standard-1-2>.
- ²⁸¹ See Committee on Economic, Social and Cultural Rights, General Comment No. 25, see note 105 above para 76.
- ²⁸² Ministry of Business, Innovation and Employment (MBIE). n.d. “Aotearoa New Zealand’s Employment Strategy.” Accessed July 22, 2026. <https://www.mbie.govt.nz/business-and-employment/employment-and-skills/employment-strategy/aotearoa-new-zealands-employment-strategy>
- ²⁸³ Pacific Data Sovereignty Trust, “About Us,” *Pacific Data Sovereignty Trust*, accessed July 14, 2026, <https://pacificdatasovereignty.com/about-us-2/>.
- ²⁸⁴ New Zealand Government Procurement. n.d. “Government Procurement Framework.” Accessed July 22, 2026. <https://www.procurement.govt.nz/government-procurement-framework/>
- ²⁸⁵ New Zealand Government Procurement. n.d. “Government Procurement Rules.” Accessed July 22, 2026. <https://www.procurement.govt.nz/government-procurement-framework/government-procurement-rules/>
- ²⁸⁶ See Government Chief Data Steward and Government Chief Digital Officer, *Algorithm Assessment Report* (Wellington: New Zealand Government, 2018), <https://data.govt.nz/toolkit/data-ethics/government-algorithm-transparency-and-accountability/algorithm-assessment-report>; and Gavaghan, Colin, Alistair Knott, James Maclaurin, John Zerilli, and Joy

Liddicoat. *Government Use of Artificial Intelligence in New Zealand: Final Report on Phase 1 of the New Zealand Law Foundation's Artificial Intelligence and Law in New Zealand Project*. Wellington: New Zealand Law Foundation, 2019. <https://www.cs.otago.ac.nz/research/ai/AI-Law/NZLF%20report.pdf>.

- ²⁸⁷ See Kingdom of the Netherlands. *Algorithm & AI Register (Register voor Algoritmen en AI)* <https://regulations.ai/regulations/RAI-NL-NA-NARANXX-2022>, a public register providing transparency about algorithms and AI used by government bodies and Government of Canada. *Directive on Automated Decision-Making* and accompanying *Algorithmic Impact Assessment (AIA)* framework, which requires impact assessments and public transparency for automated decision systems used by federal agencies see <https://open.canada.ca/data/en/dataset/fcbc0200-79ba-4fa4-94a6-00e32facea6b>
- ²⁸⁸ The International Network of AI Safety Institutes was established by Australia, Canada, the European Commission, France, Japan, Kenya, the Republic of Korea, Singapore, the United Kingdom, and the United States, in San Francisco on 21 November 2024. Affirming and building on the Seoul Statement of Intent toward International Cooperation on AI Safety Science released at the AI Seoul Summit earlier in 2024, this Network is intended to catalyse a new phase of international cooperation on AI safety see <https://digital-strategy.ec.europa.eu/en/news/first-meeting-international-network-ai-safety-institutes>
- ²⁸⁹ Department of Internal Affairs. n.d. "Media and Online Content Regulation." Accessed July 22, 2026. <https://www.dia.govt.nz/media-and-online-content-regulation>
- ²⁹⁰ See recommendation to the CEDAW committee: Te Kāhui Tika Tangata Human Rights Commission, "Report to the UN: Rights of Women in New Zealand," [tikatangata.org.nz](https://tikatangata.org.nz/our-work/submission-examination-of-aotearoa-new-zealands-9th-report-under-the-covention-on-the-elimination-of-all-forms-of-discrimination-against-women), last modified October 4, 2024, <https://tikatangata.org.nz/our-work/submission-examination-of-aotearoa-new-zealands-9th-report-under-the-covention-on-the-elimination-of-all-forms-of-discrimination-against-women>; See also Te Kāhui Tika Tangata Human Rights Commission, *Submission on the Safer Online Services and Media Platforms Proposal* (submission to Te Tari Taiwhenua Department of Internal Affairs, August 11, 2023), <https://tikatangata.org.nz/cms/assets/Documents/Submissions/2023-24-Submissions/11.08.2023-FINAL-DIA-Submission.pdf>.
- ²⁹¹ Access Matters Aotearoa, "Accessibility Legislation," [accessmatters.org.nz](https://www.accessmatters.org.nz/accessibility-legislation), accessed July 14, 2026, <https://www.accessmatters.org.nz/accessibility-legislation>.
- ²⁹² Access Matters Aotearoa, "Report Reveals Accessibility Gaps Holding New Zealanders Back" (media release), [accessmatters.org.nz](https://www.accessmatters.org.nz/report-reveals-accessibility-gaps-holding-new-zealanders-back), accessed July 14, 2026, <https://www.accessmatters.org.nz/report-reveals-accessibility-gaps-holding-new-zealanders-back>; and Access Matters Aotearoa, "Accessible Futures Summit & Parliamentary Reception," [accessmatters.org.nz](https://www.accessmatters.org.nz/accessible-futures), March 25, 2026, <https://www.accessmatters.org.nz/accessible-futures>.
- ²⁹³ New Zealand Government Chief Digital Officer (GCDO), "NZ Government Web Standards," [Digital.govt.nz](https://www.digital.govt.nz), accessed July 14, 2026, <https://www.digital.govt.nz/standards-and-guidance/nz-government-web-standards>.
- ²⁹⁴ Amy Hogan, "Why We Need a Barrier Notification System," Access Matters Aotearoa, accessed July 14, 2026, <https://www.accessmatters.org.nz/amy-hogan-why-we-need-a-barrier-notification-system>.
- ²⁹⁵ Deepfake Digital Harm and Exploitation Bill 2025 (213-1) (NZ), <https://www.legislation.govt.nz/bill/member/2025/0213/latest/whole.html>.
- ²⁹⁶ See Cassandra Mudgway, "NZ Is Criminalising Sexualised Deepfakes—Banning Apps That Make Them Should Be Next," *The Conversation*, May 18, 2026, <https://theconversation.com/nz-is-criminalising-sexualised-deepfakes-banning-apps-that-make-them-should-be-next-282127>; Hanna McCallum, "Netsafe Sees Surge in Reports of Sexual Deepfake Abuse," *Newsroom*, June 10, 2026, <https://newsroom.co.nz/2026/06/10/netsafe-sees-surge-in-reports-of-sexual-deepfake-abuse/>; Netsafe, Submission on the Deepfake Digital Harm and Exploitation Bill (2026), <https://resource.netsafe.org.nz/17-June-2026---Netsafe-submission-on-the-Deepfake-Digital-Harm-and-Exploitation-Bill.pdf>.

²⁹⁷ See Te Kāhui Tika Tangata Human Rights Commission, *Submission on Deepfake Digital Harm and Exploitation Bill* (June 18, 2026), <https://tikatangata.org.nz/cms/assets/Documents/Submissions/2025-2026-Submissions/Deep-Fakes-Bill/PDF-HRC-Submission-on-Deep-Fakes-Bill-Final.pdf>.

²⁹⁸ Ibid.

²⁹⁹ Department of the Prime Minister and Cabinet, *New Zealand's Cyber Security Strategy 2026–2030* (Department of the Prime Minister and Cabinet, February 2026) <https://www.dpmc.govt.nz/publications/new-zealands-cyber-security-strategy-2026-2030>

³⁰⁰ *Manage My Health Ltd v Unknown Defendants* [2026] NZHC 2 (interim injunction granted 5 January 2026, reasons 6 January, 2026), <https://www.courtsofnz.govt.nz/assets/cases/2026/2026-NZHC-2.pdf>; Office of the Privacy Commissioner, “Privacy Commissioner Inquiry into Manage My Health Breach,” media release, January 21, 2026, updated January 28, 2026, <https://www.privacy.org.nz/tuhono-connect/statements-media-releases/privacy-commissioner-inquiry-into-manage-my-health-breach/>.

³⁰¹ *New Zealand's Cyber Security Strategy 2026–2030* at 286 above.

³⁰² Education and Workforce Committee, *Inquiry into the Harm Young New Zealanders Encounter Online, and the Roles that Government, Business, and Society Should Play in Addressing Those Harms: Final Report* (Wellington: New Zealand House of Representatives, 54th Parliament, March 2026) <https://selectcommittees.parliament.nz/download/SelectCommitteeReport/51deb7d3-6f4c-48bb-8a93-08de7a2437b3>

³⁰³ Ibid.

³⁰⁴ United Nations General Assembly, Resolution 78/213, “Promotion and Protection of Human Rights in the Context of Digital Technologies,” UN Doc A/RES/78/213 (2023), preambular para and operative paras 15, 17 (encryption and anonymity tools “vital” to the rights to freedom of expression and privacy; restrictions must comply with States’ obligations under international human rights law). The three-part test of legality, legitimate aim, and necessity and proportionality for restrictions on encryption and anonymity is articulated by the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/29/32 (2015), para 31. OHCHR has further affirmed that encryption plays a “key role” in ensuring the enjoyment of the right to privacy and other rights: OHCHR, “The Right to Privacy in the Digital Age see note 53 above; and has recorded “the weakening of encryption” among principal state-conduct concerns: OHCHR, “Mapping Report: Human Rights and New and Emerging Digital Technologies,” UN Doc A/HRC/56/45 (2024), paras 7, 17.

³⁰⁵ Committee on the Rights of the Child, General Comment No. 25 (2021) on Children’s Rights in Relation to the Digital Environment, UN Doc CRC/C/GC/25 (2021), paras 56, 59; see also Australian Human Rights Commission, “Human Rights Explainer: Proposed Social Media Ban for Under-16s in Australia” (n.d.).

³⁰⁶ Australian Human Rights Commission, *Human Rights Explainer: Proposed Social Media Ban for Under-16s in Australia* (Australian Human Rights Commission, n.d.), https://humanrights.gov.au/_data/assets/file/0026/57752/AHRC_Social-Media-Ban-Explainer.pdf.



Te Kāhui Tika Tangata
Human Rights Commission



facebook.com/NZHumanRightsCommission



[@NZHumanRights](https://twitter.com/NZHumanRights)



[New Zealand Human Rights Commission](https://www.linkedin.com/company/new-zealand-human-rights-commission)