

Moving in parallel: Matching data and AI capability with trustworthy governance

Georgia Lala, Dr Christopher Erwin and Sir Peter Gluckman

September 2026

Liberal democracies depend on more than elections and the rule of law for their authority. They also rely on the public's continued acceptance of how their authority is exercised.¹ That acceptance rests on the expectation that governments will exercise their authority honestly and in the public interest.

Data and artificial intelligence (AI) are rapidly expanding the capabilities of government. Advances in data integration, computing power and machine learning enable agencies to design services around actual patterns of need. Agencies can detect emerging risks earlier, target interventions more precisely, reduce administrative burden and allocate public resources more efficiently.

At the same time, data and AI are reshaping the exercise of public authority. Governments can see more, know more and act earlier than ever before. These capabilities can improve public services, but they also make people, families and communities more visible to the state.

This technological transformation is occurring against a backdrop of declining public trust in democratic institutions both in New Zealand and globally.² As government capability expands, citizens will increasingly expect assurance that it is being used responsibly in the public interest.³

While New Zealand has established important foundations for trustworthy data and AI usage, governance has not kept pace with capability. Good governance makes trustworthy behaviour visible. Unless governance evolves alongside capability, the gap

¹ Weber, M. (2019). *Economy and society: A new translation* (K. Tribe, Trans.). Harvard University Press. <https://doi.org/10.4159/9780674240827>. Muller, S. H. A., Kalkman, S., van Thiel, G. J. M. W., Mostert, M., & van Delden, J. J. M. (2021). The social licence for data-intensive health research: Towards co-creation, public value and trust. *BMC Medical Ethics*, 22, 110. <https://doi.org/10.1186/s12910-021-00677-5>

² Stats NZ. (2024, September 26). *New Zealanders' trust in key institutions declines*. <https://www.stats.govt.nz/news/new-zealanders-trust-in-key-institutions-declines/>; Acumen New Zealand. (2025). *Acumen Edelman Trust Barometer 2025*. <https://acumennz.com/acumen-edelman-trust-barometer/acumen-edelman-trust-barometer-2025/>

³ Te Kawa Mataaho Public Service Commission. (2025). 2025 cross-agency AI survey: Highlights. Digital.govt.nz. <https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/artificial-intelligence/research-ai-public-service/2025-cross-agency-ai-survey-highlights>

between what governments can do and what citizens are prepared to accept will continue to widen.

Data and AI are changing how governments see, decide and act

The constitutional authority held by the state has not changed. What has changed is how that authority can be exercised. Decisions are increasingly targeted, anticipatory and, in some cases, automated. This shift in how authority is exercised fundamentally changes the relationship between citizens and the state.

On the one hand, citizens are more visible to the government than ever before through the increasing collection and use of information across public services. At the population level, the linkage of de-identified administrative data through the Integrated Data Infrastructure (IDI) in New Zealand allows the government to understand its citizens and population patterns in ways that were previously impossible. Yet in practice, people cannot meaningfully opt out of providing much of this data when accessing basic services like healthcare, schooling or income support. In Aotearoa New Zealand, this development also raises questions of Māori data sovereignty that extend beyond concerns of privacy and efficacy.⁴

On the other hand, the exercise of public authority is becoming less visible to citizens. Decisions informed by complex datasets and algorithmic tools could become difficult for administrators to explain, and for affected individuals to understand or challenge. AI further complicates this through its reliance on machine learning characterised as a black box because its inner workings are highly technical and not easily explainable.⁵ In social-support decision-making, for example, a person may be declined assistance without understanding how multiple data sources or algorithmic assessments shaped that outcome.

These developments raise the stakes for sustaining public confidence. Governments increasingly rely on citizens to provide accurate information and participate in digital services. A government that loses public confidence will find each of these tasks more difficult. This risks limiting the very capabilities that data and AI can deliver.

⁴ Kukutai, T., & Cormack, D. (2019). Mana motuhake ā-raraunga: Datafication and social science research in Aotearoa. *Kōtuitui: New Zealand Journal of Social Sciences Online*, 14(2), 201–208.

<https://doi.org/10.1080/1177083X.2019.1648304>; Brown, P. T., Wilson, D., West, K., Escott, K.-R., Babington, K., Ritchie, B., Lucas, D., Taia, I., Kusabs, N., & Keegan, T. T. (2024). Māori algorithmic sovereignty: Idea, principles, and use. *Data Science Journal*, 23, 15. <https://doi.org/10.5334/dsj-2024-015>

⁵ Choung, H., David, P., & Seberger, J. S. (2023). *A multilevel framework for AI governance*. arXiv. <https://doi.org/10.48550/arXiv.2307.03198>

Public confidence depends on trustworthy government

Data and AI will only deliver their promised benefits if citizens maintain confidence in the institutions using them. This ongoing acceptance is often referred to as social licence.⁶ Unlike democratic legitimacy, social licence is not granted once every electoral cycle. It is continuously earned as citizens evaluate whether government is acting in a way that aligns with their expectations and values.⁷

Ongoing public acceptance depends on whether citizens perceive public institutions to be trustworthy in how they exercise their authority. This highlights an important distinction between trust and trustworthiness. Where trust is a judgement made by citizens, trustworthiness is a characteristic of institutions themselves.⁸

Governments cannot simply declare themselves trustworthy.⁹ Institutions become trustworthy by demonstrating honesty, competence, and reliability: honesty in their claims and commitments, competence in executing their responsibilities, and reliability over time.¹⁰ These qualities must be visible to citizens through *actions*, rather than *assertions* of good intent.

This presents a particular challenge in an era of data and AI adoption. Trustworthiness depends on observable behaviour, yet citizens may not be able to directly observe or verify how data and AI are used and how they enable decisions.

Governance makes trustworthiness visible

Governance bridges the gap between otherwise opaque data and AI practices, the decisions they inform, and public trust by making trustworthy conduct observable. It does this through establishing clear responsibilities, public standards, and independent scrutiny. In the context of data and AI, this observability builds legitimacy. It ensures

⁶ Social licence as a term first emerged out of the mining industry in the mid-1990s to refer to the industry's need to recover its reputation after a series of public disasters. It has since been translated into a government context. See Edwards, P., & Trafford, S. (2016). Social licence in New Zealand—what is it? *Journal of the Royal Society of New Zealand*, 46(3–4), 165–180.

<https://doi.org/10.1080/03036758.2016.1186702>

⁷ Office of the Prime Minister's Chief Science Advisor. (2017, June). *Using evidence to inform social policy: The role of citizen-based analytics*. Department of the Prime Minister and Cabinet.

<https://www.dpmc.govt.nz/sites/default/files/2021-10/pmcsa-17-06-19-Citizen-based-analytics.pdf>

⁸ O'Neill, O. (2018). Linking Trust to Trustworthiness. *International Journal of Philosophical Studies*, 26(2), 293–300. <https://doi.org/10.1080/09672559.2018.1454637>

⁹ Manaaki Whenua – Landcare Research. (n.d.). *Social licence to operate framework*.

<https://www.landcareresearch.co.nz/discover-our-research/environment/sustainable-society-and-policy/slo-framework>

¹⁰ The British Academy. (2017, January). *Trust, trustworthiness and transparency* (Future of the Corporation briefing note). <https://www.thebritishacademy.ac.uk/documents/2563/Future-of-the-corporation-Trust-trustworthiness-transparency.pdf>. See Onora O'Neill's remarks.

that increasingly targeted, anticipatory and automated public power remains subject to democratic accountability.¹¹

New Zealand is not starting from scratch when it comes to data and AI governance. A growing patchwork of laws, policies, standards, and frameworks is already in place. These include the Government Chief Data Steward,¹² the Data Stewardship Framework,¹³ the Algorithm Charter for Aotearoa New Zealand,¹⁴ the Algorithm Impact Assessment toolkit,¹⁵ the Public Service AI Framework,¹⁶ the Trust Framework for Digital Identity¹⁷, and tikanga-informed guidance such as Ngā Tikanga Paihere.¹⁸ These are important foundations. The Algorithm Charter, for example, was introduced to improve consistency, transparency and accountability in government use of algorithms.

However, these mechanisms do not yet form a coherent assurance system. New Zealand's current patchwork establishes expectations and guidance, yet much of the responsibility for interpretation and implementation remains within individual agencies and relies heavily on self-assessment. Indeed, the independent year-one review of the Algorithm Charter identified that agencies have largely been left to interpret and implement charter commitments themselves.¹⁹ A system of self-design, self-assessment and self-auditing is not defensible if the goal is to maintain social licence.

These gaps point to the need for a more mature assurance model grounded in independent scrutiny. Independent assurance strengthens the overall system by providing confidence that powerful capabilities are being exercised with clear boundaries and subject to meaningful accountability. When data and AI systems

¹¹ New Zealand Government. (2022). *Data and Statistics Act 2022*. New Zealand Legislation. <https://www.legislation.govt.nz/act/public/2022/39/en/latest/#LMS418574>; Bovens, M. (2007). Analysing and assessing accountability: A conceptual framework. *European Law Journal*, 13(4), 447–468. <https://doi.org/10.1111/j.1468-0386.2007.00378.x>

¹² Stats NZ. (n.d.). *Government Chief Data Steward*. Data.govt.nz. <https://data.govt.nz/leadership/gcnds>

¹³ New Zealand Government. (2020, November 18). *A data stewardship framework for New Zealand*. Data.govt.nz. <https://www.data.govt.nz/toolkit/data-stewardship/a-data-stewardship-framework-for-nz/>

¹⁴ New Zealand Government. (2023, June 15). *Algorithm Charter for Aotearoa New Zealand*. Data.govt.nz. <https://data.govt.nz/toolkit/data-ethics/government-algorithm-transparency-and-accountability/algorithm-charter/>

¹⁵ New Zealand Government. (2023, December 18). *Algorithm Impact Assessment toolkit*. Data.govt.nz. <https://data.govt.nz/toolkit/data-ethics/government-algorithm-transparency-and-accountability/algorithm-impact-assessment-toolkit>

¹⁶ New Zealand Government. (2025, January 29). *Public Service Artificial Intelligence Framework*. Digital.govt.nz. <https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/artificial-intelligence/public-service-artificial-intelligence-framework>

¹⁷ Department of Internal Affairs. (2024, September 19). *Trust framework for digital identity*. NZ Digital government. <https://www.digital.govt.nz/standards-and-guidance/identity/trust-framework>

¹⁸ Stats NZ. (2020). *Ngā Tikanga Paihere: Guidelines for responsible data use*. Data.govt.nz. <https://data.govt.nz/assets/data-ethics/Nga-Tikanga/Nga-Tikanga-Paihere-Guidelines-December-2020.pdf>

¹⁹ Taylor Fry. (2021). *Algorithm Charter for Aotearoa New Zealand: Year 1 review*. Stats NZ. <https://www.data.govt.nz/assets/data-ethics/algorithm/Algorithm-Charter-Year-1-Review-FINAL.pdf>. See Theme 6.

influence public services, public assurance requires more than agencies demonstrating their own compliance.

An independent data and AI oversight body

Bearing this in mind, New Zealand would do well to consider an independent data and AI oversight body.²⁰ With a statutory mandate across government, an oversight body could independently review high-impact uses of data and AI, provide assurance over agencies' use of impact assessments, maintain a public register, publish independent findings, and recommend that harmful uses be corrected, paused or stopped.

An independent oversight body need not replace the defined roles of the Privacy Commissioner, Ombudsman, Stats NZ or Māori data governance. Its purpose would be to provide an additional layer of public assurance. Properly designed, an oversight body could help ensure that expanding capabilities meet citizens' expectations without slowing responsible innovation. New Zealand needs independent and consistent data and AI oversight capable of operating across all of government.

New capabilities must be matched by stronger public assurance. Data and AI will continue to expand what governments can see and do. But capability alone does not determine whether public value will be delivered. A system may be technically sophisticated and legally compliant yet fail to meet citizens' expectations if its decisions are difficult to understand or challenge.²¹

Expanded government use of data and AI is inevitable. But the success of these technologies depends on more than what governments can do with them; it depends on whether citizens trust how they are used. Capability and governance must now move in parallel.

²⁰ Office of the Prime Minister's Chief Science Advisor. (2019). *Citizen-based analytics* (PMCSA report No. 17/06/19). Department of the Prime Minister and Cabinet.

<https://www.dpmc.govt.nz/sites/default/files/2021-10/pmcsa-17-06-19-Citizen-based-analytics.pdf>

²¹ Green, B. (2022). The flaws of policies requiring human oversight of government algorithms. *Computer Law & Security Review*, 45, 105681. <https://doi.org/10.1016/j.clsr.2022.105681>