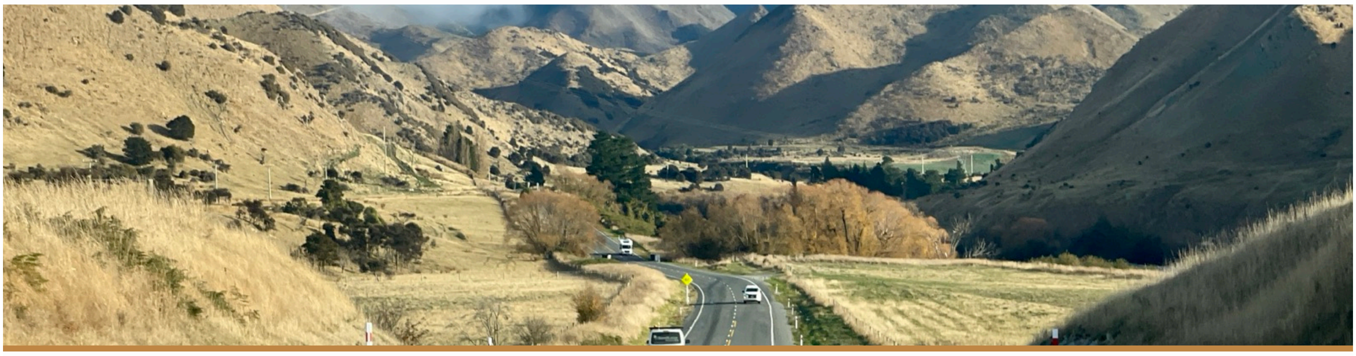


Making policy bite

Version 0.1 · revised 7 September 2026 · this version as a PDF

> Drafted with AI assistance, then checked and revised by the author. The judgements and the errors are the author's.

What government can actually do, and why most of what it does changes nothing.

Series part J · Version 0.1 · August 2026

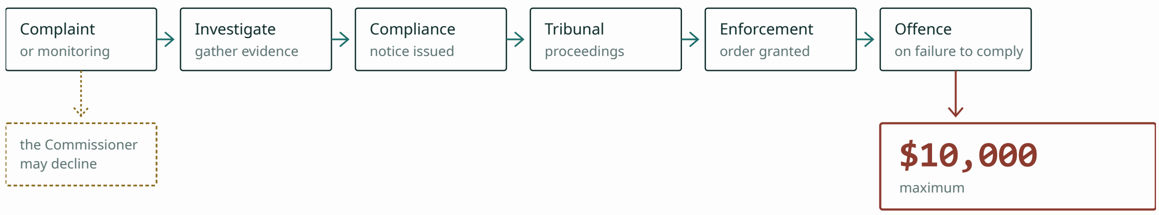
The question officials are never asked

Most argument about technology policy is about *what the rule should say*. Almost none of it is about what happens after the rule says it.

That is the wrong emphasis, and New Zealand has a domestic demonstration of why.

What the Privacy Act shows

FIG-13 EVERY LINK WORKS · PRIVACY ACT 2020



Nothing in the chain is missing. It reaches overseas companies doing business here.
It ends in a sum a firm with revenue in the hundreds of billions treats as an administrative cost.

Enforceability is not a property of the text. It is a property of the mechanism behind it —
and a chain is only as strong as its last link, which is where nobody looks.

FIG-13 The Privacy Act 2020 enforcement chain, complete and carefully drafted, terminating in a ten thousand dollar maximum. The Act does not fail because it is badly written. It fails because the last link is not heavy enough.

The Privacy Act 2020 was presented as strengthening privacy protection and enhancing the Commissioner’s role. It has a complete enforcement chain, and each link works:

1. A complaint is made, or the Commissioner acts on monitoring. **The Commissioner may decline to investigate.**
2. The Commissioner investigates and gathers evidence.
3. The Commissioner issues a compliance notice — do this, stop that, by this date.
4. The notice may be published where publication is in the public interest.
5. If it is ignored, enforcement proceeds in the Human Rights Review Tribunal.
6. The Tribunal grants enforcement orders and costs.
7. Failure to comply with an enforcement order is an offence, punishable by a fine of **up to ten thousand dollars.**

Nothing in that chain is missing. It was carefully drafted. It reaches overseas companies doing business here, which is more than many countries’ laws manage. And at the end of it sits a number that a firm with revenue in the hundreds of billions would process as an administrative cost.

The Act does not fail because it is badly written. It fails because the last link is not heavy enough to hold the chain.

That is the lesson worth taking into any AI policy. Enforceability is not a property of the text. It is a property of the mechanism sitting behind the text, and the mechanism has to be examined link by link, because the chain is only as strong as the weakest one — which is nearly always the last one, and occasionally the first.

Walking a duty to its end

For any obligation a government is considering, six questions. If any one of them has no clean answer, the obligation is decorative.

Who exactly is obliged? Not “providers” or “agencies” — a class of person a lawyer could serve papers on.

Who checks? A named body, with a budget line, and the technical capacity to know what it is looking at. An audit right exercised by nobody is a form.

What can they compel? Documents, systems access, a demonstration, an expert’s report. A regulator who may ask questions and cannot compel evidence is dependent on the goodwill of the party under investigation.

What happens when the answer is no? Not what *may* happen. What has happened, in comparable cases, on average.

Who bears the cost of finding out? If detection depends on a harmed party noticing, complaining, and persisting through a tribunal, the obligation binds only where someone is willing to spend two years on it.

And how would we know it is working? A published number. Notices issued, proceedings brought, outcomes. Where nobody counts, nobody knows, and an unenforced duty is indistinguishable from a well-observed one.

Applied to the Privacy Act, that walk terminates at question four. Applied to New Zealand’s current AI instruments — a Cabinet paper, a strategy, a public service framework — it terminates at question one, because none of them creates an obligation on anyone.

Three roles, and one that is not on the list

FIG-07 THREE AMENDMENTS TO INSTRUMENTS ALREADY IN FORCE

IN FORCE TODAY		AMENDED	COST
“…where a suitable onshore service exists” undefined; a region satisfies it	→	Suitability defined by the two-part sovereignty test	nil
Cloud Jurisdictional Risk guidance (2024) advisory to a risk assessment	→	Operator compulsion becomes a mandatory, evidenced element	nil
No on-premise investment without GCDO approval	→	Sovereignty-qualifying infrastructure is not on-premise investment	nil

FIG-07 Three changes to instruments already in force. Five of the seven policy proposals cost nothing; these three cost nothing and need no legislation.

Government has three distinct levers here, and confusing them is why capable people produce policy that does nothing.

Legislator

Creating obligations that bind. The hard part is not drafting; it is the consequence at the end of the chain, and the will to set it at a level that changes a commercial calculation rather than registering disapproval.

Two obligations in this domain would matter more than the rest:

A prohibition on public-sector data entering vendor training, rather than a disclosure regime. The reasoning is irreversibility: data used to train a model cannot be withdrawn from it. Where harm cannot be undone, remedies applied afterwards are decoration, and only a constraint applied beforehand does any work. This is not contested by anyone technical.

A declaration requirement for AI in the software supply chain — whether a product performs inference, which model, operated by whom, in which jurisdiction, under what data terms, with notice on material change. This is a bill of materials extended from security to the inference path, and the security equivalent went from novel to standard within a few years.

Buyer

This is the underweighted lever and it needs no legislation.

A supplier who wants Crown revenue meets the Crown's conditions. That is faster than statute, cheaper than a regulator, and it reaches the private sector indirectly because suppliers do not maintain two product lines.

New Zealand already has the instruments. Cloud First is live and refreshed in 2023, and it carries provisions that would do real work if they were sharpened:

- It provides that RESTRICTED information should over time be held in a New Zealand data centre **where a suitable onshore service exists** — a term we have not found authoritatively defined. Define it as *data here, and an operator beyond foreign compulsion*, and a dormant sentence becomes the strongest sovereignty provision in New Zealand procurement.
- Cloud Jurisdictional Risk guidance, updated in 2024, informs a case-by-case assessment. Make operator compulsion a mandatory and evidenced element, such that an assessment considering only data location is non-compliant.
- Agencies must implement a multi-cloud approach avoiding over-dependence on any single supplier — portability, already policy, never enforced against the dependency that matters.

- Agencies must consider te ao Māori perspectives for Māori data, with guidance in development.

None of that requires a bill. Two of them are the government's own commitments, unenforced.

There is also a restriction working directly against the grain of this series: public service agencies and some Crown entities may not invest in on-premise infrastructure without meeting specified criteria or obtaining approval. That rule predates affordable local inference. Infrastructure meeting a sovereignty test should not count as on-premise investment for its purposes.

Enabler

The things only government can do, because they need either independence or a mandate longer than any company's life.

The clearest example is **a timestamp authority**. A timestamp proves that a record existed in a particular form at a particular time — and it is worth nothing unless issued by a party with no interest in the record. That makes it infrastructure rather than a product: any company operating one for its own customers has recreated the problem it claims to solve.

This is not speculative. The New Zealand Information Security Manual has carried post-quantum guidance since January 2022, and version 3.9 records that quantum developments can undermine all widely used public key algorithms for digital signatures, and that historical and archived data may be at risk. Migration protects records written from now on. Records already signed become *retroactively forgeable* — and cannot be re-signed, because the people and organisations that signed them may no longer exist.

Archives New Zealand holds the Public Records Act mandate for the digital record of government, and its own long-term strategy anticipates that not all records of enduring value will be transferred to the archive, and that technology will provide methods of assuring authenticity of records whether archived or in current use. That is a description of what a timestamp authority does. The strategy names the requirement; nothing published names the mechanism.

A timestamp authority is small. It receives fingerprints and returns signed tokens; it holds no records and sees no content. The difficult parts are institutional: key custody, a published renewal policy, continuity across decades, and standing in evidence — because a timestamp nobody is obliged to accept is a service nobody will use. The legislative work and the operational work have to move together.

And not: operator

The reflex answer to any capability gap is that the Crown should build it. It should not, and the reason matters.

Sovereignty achieved by dependence on the Crown is dependence that has been re-domiciled, not removed. A 2029 government can defund it. An agency can deprioritise it. The organisations relying on it have exchanged a foreign vendor they cannot refuse for a domestic one they cannot vote out between elections.

Where capability is needed, the better instrument is **anchor tenancy**: a multi-year service commitment open to any operator meeting the standard. More bankable than a grant, ordinary procurement rather than novel structure, survives a change of government better than a line item, and it leaves the Crown out of the governance of the things it buys from.

Where capital is genuinely required, it should be redeemable, time-limited, and carry no special governance rights.

The one thing government should not do for this blueprint

Not fund it. Not found it. Not prefer it.

The blueprint in this series is published for anyone to build from, and it is worth exactly as much as its independence. A commons pattern that quietly asks for support has stopped being a commons pattern.

What government can usefully do is make the conditions under which anyone can build it: define the test, make jurisdictional risk bind, remove the on-premise obstacle, establish the timestamp authority, and buy from whoever meets the standard.

That is a smaller ask than a programme, and it is the one that survives an election.

Where this currently stands

New Zealand has an AI strategy from MBIE that emphasises adoption over foundational development, a 2024 Cabinet paper reasoning that existing law provides guardrails and that a standalone AI Act is not preferred, and a public service framework. All three are deliberately light-touch. There is no AI-specific legislation and none has been tabled.

None of that is a failure of intent. It is what happens when the question being asked is *what should the rule say* rather than *what happens after it says it*.

Sources and what we could not establish

The Privacy Act chain above is drawn from the Act and from published legal analysis; section references should be checked against the Act itself before anyone relies on them.

Three things we could not establish and did not assume. **Whether a transfer prohibition notice has ever been issued** — that power is the strongest cross-border provision in the Act and, if it has never been used, that fact is more telling than anything else in this essay. **How many compliance notices have been issued since 2020 and how many reached the Tribunal.** And **how New Zealand's penalty ceiling compares with other jurisdictions'** — the comparison is the obvious rhetorical move and we have not verified the numbers, so we have not made it.

If you can supply any of the three, this essay is better corrected than defended.

▶DISCLAIMER

Cite this version

```
Making policy bite, version 0.1 (September 2026).
agenticgovernance.digital/downloads/making-policy-bite-v0-1.pdf
```

PREVIOUS
I · What actually stops an AI doing the wrong thing

Series contents