

AN ALTERNATIVE TO BIG TECH AI · ESSAY 4 OF 7

Your Model, Your Walls

For teams who can't put sensitive material in someone else's cloud: an AI that runs inside your own walls and never phones home.

Work that can't leave the room

For sensitive work, "it's in the cloud" is the problem stated politely.

- Counselling notes, case files, board strategy, patient records can't be a window someone else watches through.
- It's the architecture, not a mis-set toggle — the data has to leave for a cloud model to read it.
- These teams don't need a better promise about data that left; they need it not to leave.

Where "the cloud" actually takes your data

A cloud AI feature reads your text by sending it out of the building.

- It sits on a few large companies' infrastructure, reachable under foreign law wherever you are.
- Your text may be retained, reviewed, or shape the next version of the model.
- The disqualifier is "can I account for everywhere this has been" — and the answer breaks.

A model inside your walls

The Village runs the model where the data already is — no call to OpenAI, Google or Anthropic.

- A modest ~14B open model, fine-tuned per community, served on self-hosted inference.
- June 2026: the external-AI consent path was removed; the audit log records only the Village's own engine.
- "The data doesn't leave" is now a property of the software, not a promise — there's nowhere for it to go.
- Honest bound: not claiming to out-think frontier models; the win is custody, not raw IQ.

Situated, not averaged

A model that only sees your kind of work gets the particulars a global average smooths away.

- Frontier models are built to be everyone's — which makes them, in the particulars, no one's.
- Yours is tuned to your context and runs under your own rules.
- None of those particulars ever become someone else's training data.

How far into your walls you can pull it

Choose how thick the walls are — up to the whole thing on hardware you own.

- Shared-but-partitioned → a dedicated database → fully self-hosted on your own premises.
- Hub-and-spoke: members reach only the moderators helping them — for counselling, case management, mentoring.
- Your logo, colours, vocabulary, domain and mail — it looks like yours because it is.

Who needs walls this thick

Most don't; the ones who do know exactly who they are.

- Security-minded teams inside larger organisations who know "it's in the cloud" isn't an answer.
- Counselling and hauora services whose duty of confidence is the basis of the work.
- Boards with commercial-sensitive or privileged matters; units answerable to a regulator.

See it for yourself

- The demo Villages — mysovereignty.digital/demos.html
- The free Governance course — mysovereignty.digital/course.html
- Read the essay — agenticgovernance.digital/papers/your-model-your-walls.html

You don't have to choose between Big Tech AI and no AI. You can hold your own.