New Title

If money didn’t exist, the best digital infrastructure would optimize for **meeting needs, using resources well, and giving people meaningful control**—not for revenue, growth, or monetizing attention. Scarcity would still exist, so the system would need transparent ways to coordinate labor, energy, equipment, and priorities without turning those measures into money.

A strong design would be **federated**: communities operate their own infrastructure, while shared protocols let them cooperate across regions.

- **Community-owned networks:** Local mesh and fiber networks, public Wi-Fi, and community-run data centers, connected to regional and global backbones. Networks should keep working locally when outside connections fail.
- **Shared, open foundations:** Open-source operating systems, communication tools, identity standards, data formats, and APIs. People should be able to move between services without losing their data or contacts.
- **Local control with coordination:** Neighborhoods, towns, and larger communities set their own rules and priorities. Federations coordinate things that need broader scale—such as scientific research, disaster response, translation, and global infrastructure—without requiring one organization to own everything.
- **Privacy-preserving identity:** People can prove relevant facts—such as eligibility or community membership—without exposing their full identity or creating a universal tracking profile. Essential services should not require intrusive identification.
- **Distributed, resilient computing:** Store and process data near the people who need it, with encrypted backups across independent communities. Use central facilities where they are efficient, but avoid making any one provider or location a point of failure.
- **Useful, non-market coordination:** Shared inventories and planning tools could show available equipment, energy, skills, and unmet needs. Decisions should combine local input, expert knowledge, ecological limits, and transparent public priorities—not reduce every choice to a single numerical score.
- **Democratic governance and safeguards:** People affected by a system should have a say in its rules. Administrators need limited powers, auditable decisions, appeal processes, and protections against surveillance, exclusion, and capture by a technically skilled minority.
- **Accessibility and offline operation:** Services should work on low-cost devices, support assistive technologies and many languages, and provide local or offline access during outages.

The key tradeoff is **local autonomy versus shared coordination**. Make decisions locally when their effects are local; coordinate at larger scales when networks, ecosystems, or shared resources cross community boundaries. Decentralization should mean that communities can operate, govern, and leave systems—not merely that data is copied across many servers.

In short: **a public, federated digital commons**—community-operated where possible, interoperable by default, resilient in failure, and governed by the people who rely on it.

There wouldn’t be one ideal number. The right number depends on population, geography, power supply, network capacity, and how much service must continue during outages. I’d design a **layered system**, with the smallest practical number of large facilities and enough local capacity that communities aren’t helpless when links fail.

Layer	What it should host	Approximate role
Large regional data centers	Heavy computing, large shared datasets, training and scientific workloads, long-term backups	A small number per large geographic region, connected to multiple independent power and network routes
Community or edge data centers	Local copies of essential services and data, local search, communications, caching, public-service applications	At least one per community or cluster of communities where losing the wider network would seriously disrupt daily life; larger areas may need several
On-premise servers	A hospital’s clinical systems, a school’s local services, a municipal control system, a factory’s operations	Used when low latency, privacy, or the ability to operate through a network outage matters; coordinated with wider services rather than isolated
Home self-hosting	Personal files, small websites, experiments, household backups, services for a small group	Optional, supported by easy tools; not the default place for critical public services or the only copy of important data

A practical rule is to size facilities by **failure boundaries, not just population**. Each community should be able to keep a basic set of services running without the regional internet: local messaging, emergency information, identity or access services where needed, essential records, and access to cached learning and reference materials. Critical services should have another copy in a physically separate location, ideally on a different power and network path.

That argues for **many modest edge sites, not a tiny number of giant hubs—and not a server in every home**. Home hosting can add experimentation and personal control, but household connections, hardware, backups, and maintenance are uneven. It shouldn’t become an unspoken requirement for participation, nor should a person’s home server become a single point of failure.

The design should also avoid duplicating everything everywhere. Keep frequently used and time-sensitive services close to people; put specialized, compute-intensive work in shared regional facilities; replicate critical data across independent sites; and let local systems synchronize when connections return. Measure success by service continuity, energy and materials used, latency, accessibility, and community control—not by maximizing server count.

Revision #1
Created 2026-11-10 21:39:05 UTC by Dennis Paassen
Updated 2026-11-10 21:39:54 UTC by Dennis Paassen