Who Owns What the Network Knows About You

A review of eight articles on the architecture of an open 6G. For readers who do not work in telecommunications.

Two Questions

You have never chosen how communication works. You chose a tariff, a phone model, sometimes an operator. The architecture - never. It was chosen for you long before the purchase, by people you never saw, in rooms you were not invited to.

Right now such a room is at work again. The 6G standard is being written in these very years, and whatever gets into it will reproduce itself for the next twenty years - through equipment, through regulation, through the habits of billions of people. The eight articles discussed here were written from inside that work and addressed outward: to those who are not in the room.

A word on timing first, so that the rest reads calmly. This is not about tomorrow. The first stage of the standard freezes in March 2027, the second in June 2028, full specifications are expected in early 2029, the first commercial networks around 2029-2030, mass-market consumer devices later still. The window really is closing, but it has a specific date rather than a feeling of haste.

All eight articles answer one question:

> **Who owns what the network knows about you and does for you - and can communication be arranged so that this stays closer to you than to the center?**

You have your own question, derived from that one. This review exists for it:

> **If all this is true - what is in it for me, and in what case do I not need it?**

The answer to the second comes at the end, and it is not a one-word answer.

Eight Locks on One Door

The image running through the series is distance. Each article takes one thing and asks whether it lies near you or far away.

1. A Network With No Owner. An ant colony. No single ant governs the colony, and yet the colony finds food. The pheromone trail is not in the ant's head and not on a server - it lies in the environment, and it evaporates unless it is reinforced. The conclusion: a network can have no owner not because that is fairer, but because in a distributed architecture there is nothing to own. Nature has been testing this scheme for a hundred million years.

2. A Trail in the Protocol. How to reproduce it technically. A data packet passing through a node leaves a mark: how long this hop took, how much was lost. The next packet reads the fresh marks and picks its road. Memory of the network's state accumulates in the network itself rather than in an operator's table. Something similar already partly works - in the OSPF, MPLS and QUIC protocols, in research algorithms of the AntNet family. None of these solutions has been carried through to the end.

3. The Center That Should Not Exist. For whom. A doctor in a small district town, three hours' drive from the nearest base station, because building one there is commercially unjustifiable. A patient's sensor sends an alarm through a chain of seven neighboring devices, not one of which belongs to an operator. A network appears where there are devices. Devices are where there are people.

4. Three Lines in the Standard. What exactly to write in. A mandatory field in the packet header, no more than 16 bytes: last-hop delay, loss ratio, timestamp. An open format for that field, so that one manufacturer's device can read another manufacturer's mark. And a signature from a protected chip - because an ant cannot lie about a trail, but a node can.

5. The Question That Must Be Asked. Where this is decided. Not among engineers - among those who allocate the money. The question runs: what will a specific person get from 6G that they do not have now? A centralized architecture has no answer. Whoever lives inside the commercially viable zone will get the same thing, only faster. Whoever lives outside it will get nothing. Just as now.

6. A Lock With No Single Key. Trust and the wallet. The lock has no key at all - not a thick one, not a hidden one, not one cut into pieces. It opens to a chord of four independent confirmations: the device's chip, geometry (the network measures position to centimeter accuracy from several separated points at once), neighboring devices belonging to strangers acting as witnesses, and the living presence of a human being. No single note opens the lock alone, and no two of them rest on a shared foundation. A software agent is issued not a key but an errand with an expiry: three actions, one amount, forty minutes.

7. The First Node. Where it all begins. You bought the first such device, switched it on - and nothing. Not because it is broken. Because there is no one to talk to. Connectivity does not appear gradually but in a jump: while the average number of neighbors within range is below roughly 4.5, long paths do not exist. Not worse - they do not exist. There is no intermediate state. And almost nobody will change any setting: a device does whatever it was shipped doing, for its whole life.

8. A Network With No Owner, A Reflection With One. The most uncomfortable article; it partly refutes the preceding ones. The radio signal a network uses to carry data also, incidentally, measures whatever it bounced off. Wide bandwidth is needed for speed - and the same bandwidth distinguishes distances to about one and a half centimeters. At 300 GHz the wavelength is one millimeter, while the chest wall moves 4-12 millimeters when breathing and the skin moves up to half a millimeter with each heartbeat. This cannot be declined: it is not a feature somebody added but a property of transmission itself.

Here a bound is required, without which the previous paragraph sounds more frightening than it is. A single measurement is a shapeless blur; nothing follows from it. To obtain an image, a gait, or a breathing rate, measurements must be **accumulated with coherent phase**: an image takes hundreds of milliseconds, breathing and pulse take seconds. Communication, meanwhile, needs a window shorter than a tenth of a millisecond. The same holds in space: data transmission needs nodes to agree in time to within nanoseconds, whereas joint imaging needs agreement in phase, that is, to fractions of a picosecond. Three orders of magnitude in both cases, and only one of them is required for the link to work. Hence the whole principle of the article: **do not forbid measurement, remove accumulation.**

And a second correction to the scale of the alarm. None of this is appearing for the first time. Radar that reads breathing already sits on bedside tables; modules that detect a pulse through a blanket sell for a couple of hundred euros; the standard for sensing over ordinary Wi-Fi was published in 2025. What is new in 6G is not the capability but the fact that measurement stops requiring a separate instrument, bought and aimed by whoever wants the result, and becomes a by-product of data transmission by infrastructure that stands there for another reason.

But the same physics has a side that favors you. A reflected signal weakens with distance twice over - out and back. The instrument on your body is centimeters from your skin; a network node is meters away. **Nobody is closer to you than you are.** This is not a right that someone grants. It is geometry, and a standard can only preserve it or spoil it.

Something You Already Know From Your Own Life

Here the series meets something familiar to anyone.

You almost never change default settings. Not because you do not care, but because there are too many of them and you have one life. Behavioral economics has measured this on pension plans, on organ donor consent, on subscriptions: the share of people who change a factory setting is almost always small. A caveat is mandatory: those measurements come from other domains, and transferring them to communication settings is a plausible assumption rather than an established fact. In the donation case the gap between countries is considerably larger in declared consent than in the actual number of transplants.

The seventh article says the same thing about devices, more drily: owners weigh nothing, because switching between "I am an endpoint" and "I am a relay" happens automatically, and whatever the device left the factory with was set by whoever configured it.

The fifth article reaches the same conclusion from another direction: the structure of the room determines the structure of the questions. Engineers in working groups solve real problems and intend no harm - it is simply that the network their employer builds has to be commercially viable, and viability requires a center. The center reproduces itself not by malice but by arithmetic.

Two different sciences, one conclusion. **The decision is already being made for you, and not at the moment you buy a phone.**

What You Get If This Is Done

Four things, each checkable against your own experience.

Coverage appears where it is unprofitable. Not through an operator's kindness, but because your phone and the phones around it become the network themselves. A country house, a highway, mountains, a village, an old building with thick walls.

A stolen phone stops being a catastrophe. There is no key in the wallet that can be carried away: no password, no seed phrase, no file. The next day, with a new device, access is restored, because your identity did not live in the phone.

A network cannot hand over what it does not remember. The requirement is not phrased as "forbid measurement" - that is impossible - but as "remove the ability to accumulate." The difference is decisive: a promise not to collect cannot be verified from outside, whereas the absence of the capability sometimes can be.

Your own instrument reads you better than the infrastructure does. By geometry, not by anyone's permission.

Honestly: When You Do Not Need This, and What It Costs You

This section is largely the series arguing against itself, and that is its strength.

If you live in a large city, you personally probably do not need this. You are already inside the commercially viable zone. You will have coverage under any scenario, just faster. The whole advantage goes to whoever lives not where a network is profitable but where it is needed.

A dense ownerless network sees you better than a sparse operator network. The eighth article does the arithmetic honestly: doubling the number of nodes per unit area eats about six decibels of the margin that protects you, and along a street, which is exactly where relays get installed, twice that. A caveat: this holds all else being equal, and all else is not quite equal - nodes in a dense network operate at lower power, and part of the loss comes back. But the direction is as stated: the architecture the series argues for across seven parts turns out, in the eighth, to be the better observer.

Other people's packets will pass through your device. That means battery, heat and traffic. The series answers that the mode switches automatically according to conditions, but it does not promise this is free.

Until there are neighbors, what you hold is a useless object. Below the threshold the network does not work badly; it does not exist. Somebody has to buy the first devices and keep them switched on for years inside an empty network.

Protection remains a possibility, not a guarantee. The advantage of proximity works only if the instrument is on you. Wearables get taken off, forgotten, left on the charger - most often by exactly the people for whose sake the section on saving lives was written. A standard can preserve the advantage. It cannot make a person use it.

And the most sober point: this is not the only road. Intermediate, partly decentralized architectures exist - they are better than pure centralization, although for the doctor in the third article a hybrid changes little: if the station is unprofitable, it will not appear. But his problem has other solutions too, which the series barely mentions: direct satellite links to an ordinary phone, coverage obligations attached to licenses, direct subsidies, community networks. The series' argument does not collapse because of this - but it turns from "the only way out" into "one of the ways," and that is more honest.

What You Can Actually Do

Less than one would like, and more than it seems.

You personally will not write a line into the standard and will not attend a working group meeting. But the question that is not asked in that room is a simple one, and it can be put by anyone who has someone to put it to: **explain concretely what a person outside the zone of commercial viability will get from this architecture. Not on average across urban coverage - for him.** The centralized answer to it does not exist. There is silence, and the silence is itself an answer.

The second thing matters more and is almost always missed. This is not a game where you are against the operator and someone necessarily loses. The eighth article shows why giving up the capability benefits the side normally treated as the opponent. A network able to reconstruct the interior of rooms is obliged to store that capability, defend it, and produce it on demand in every jurisdiction where it operates. It will be asked for. It will eventually be breached. Someone will have to answer for it. An operator structurally incapable of forming the image cannot be compelled to hand it over, cannot lose it, and cannot be held liable for it. **Incapability here is a form of protection for the party deprived of it.** This is the rare case where a cautious architecture benefits both sides rather than being won from one of them.

And the third: remember that participation in the network is a factory setting, not your choice. The argument is not about how to persuade device owners. The argument is about who is allowed to set that default.

In Closing

You have never chosen how communication works. That will not change: even in the best case you will configure nothing, read no working group document, and never learn the word "quorum."

Something else will change - distance. Memory of paths will lie in the network rather than on someone else's server. Trust will be spread across several foundations rather than stacked in one point. What can be measured about you will stay closer to you than to the infrastructure.

So whether you personally need a new communication protocol depends on where you live, what you wear on your body, and how many years ahead you are counting. But the question of who all this will belong to is being decided now, once, and for a long time.

Nobody is closer to you than you are. For as long as that is true by geometry rather than by someone's permission.

Appendix: Article - What It Gives You Personally

Article	About	What it means for you
A Network With No Owner	An ant colony as proof	A network can have no master - technically, not ideologically
A Trail in the Protocol	The mark inside the packet	The network itself remembers where the link is good, with no operator server
The Center That Should Not Exist	The doctor in the district town	Coverage appears where people are, not where it is profitable
Three Lines in the Standard	Field, format, signature	Devices of different brands understand each other and cannot lie
The Question That Must Be Asked	Whom to ask	Your interest is not represented in the room - and the cause is structural, not malicious
A Lock With No Single Key	A chord instead of a key	A stolen phone does not open your life; there is nothing in it to steal
The First Node	The neighbor threshold	Until the network exists the device is useless; the factory setting decides
A Network With No Owner, A Reflection With One	Your reflection	The network measures you incidentally; what protects you is distance and the absence of accumulation, not a prohibition

---

An ant does not know it is building a road. It follows a trail left by someone before it and leaves one of its own - and out of this, with no design behind it, comes the path the whole colony will take.

Communication standards are written in much the same way, only slower, and by people instead of ants. Nobody holds the whole in mind; each leaves a mark, and the mark survives for as long as it is reinforced.

These eight articles are one such mark. What comes of it depends on whether anyone walks the same way after.