A Network With No Owner, A Reflection With One

Part Eight of the series on the architecture of open 6G

A 6G network does not need to be fitted with sensors in order to watch you. It watches because it works. This is not a warning about what engineers might one day add; it is a description of what the physics already does, in every node, in every packet, without anyone deciding it.

The standards bodies have noticed. 3GPP's feasibility study on integrated sensing records that such a network can follow micro-movements including heart rate, and that at sufficient resolution the results could amount to visual profiles of people. ETSI has a group studying privacy mechanisms for exactly this, and the research literature has been describing the problem since at least 2022. The problem is on the table. What is on the table with it is the wrong instrument: every remedy so far proposed is a data protection remedy - consent, lawful basis, encryption, authorisation. In this specific domain those instruments do not merely underperform. They do not apply, for a reason that is structural rather than political.

The seven previous parts of this series argued about ownership: of the infrastructure, of the network's memory, of the trust roots, of the observations neighbours exchange. This part is about something that was never anyone's to own, and that is now, quietly, becoming somebody's.

Your reflection.

What the physics decided for us

Faraday spent six lectures on a burning candle, and beneath all of them lay one lesson: a candle does not give heat and also give light. It gives one process, seen from two sides. You cannot order the heat without the light.

Communication above 100 GHz is a candle of this kind. Three ordinary facts, each harmless alone.

Resolution. How finely a radio system distinguishes distance depends on its bandwidth. A 6G channel is wide because wide is fast. But the same width that carries the data resolves distance to roughly a centimetre and a half. Nobody chose that. It arrives with the speed and cannot be declined.

Phase. At 300 GHz a wavelength is one millimetre. A chest wall moves four to twelve millimetres with each breath; the skin moves up to half a millimetre with each heartbeat. Against a one millimetre ruler, a heartbeat is not a measurement at the edge of the noise. It is a full swing of the needle.

It would be convenient to claim 6G introduces this. It does not. Radar that reads breathing already sits on bedside tables, and modules advertising heart rate to within one beat per minute, through bedding, sell for a couple of hundred euros. What those need is a dedicated sensor, aimed and

placed by the person who wants the measurement. That is precisely what 6G removes. Measurement stops requiring a device bought for the purpose and becomes a by-product of carrying data, performed by infrastructure that is there for another reason, on people who did not install it. The change is not in what can be measured. It is in **who has to intend it**.

Aperture. A single array in a handset is small, and small apertures see blurred shapes. But the architecture 6G requires in order to work at all - relays that preserve phase, nodes synchronised by atomic clocks, arrays cooperating as one distributed antenna - is, in the language of radio astronomy, an interferometer. Ten nodes along a street, sharing a phase reference, form an aperture the size of the street. A blur becomes an outline.

This third one is a projection, not a report: phase coherence across metres at a millimetre wavelength is undemonstrated at network scale. It belongs here because the architecture is being designed to make it possible, and design decisions are what a standard governs. A second honest limit cuts against the alarm: at these frequencies walls are close to opaque and range is short, so sensing is largely line-of-sight. What matters is the indoor case, where the nodes are inside with you. Through-wall is mostly a distraction.

And beneath all three sits a fact impossible to work around. Every receiver, in every digital radio system ever built, must estimate the channel before it can decode anything - how the signal was delayed, bent, absorbed and echoed on the way in. That estimate is not an optional diagnostic. It is the precondition of reading the data at all. At the bandwidths of 6G, that mandatory estimate is a description of the room.

So the network does not collect information about you as a separate activity that could be switched off. It cannot decode your message without first measuring the space you are standing in. Asking for 6G connectivity without sensing is asking for flame without light.

Why consent does not apply

Every instrument we have for protecting privacy rests on one silent assumption: the data comes *from* the person. They type it, send it, agree to it. From that follows the whole toolkit, and all of it operates at the moment of transmission.

Reflection removes the assumption. Here the data does not travel from the person; it is **manufactured by the receiver** out of physics. There is no key they hold, nothing to encrypt, nothing to decline to send, no moment of transmission to which a permission could attach.

This is not consent being weak, or poorly informed, or buried in a dialogue box. It is consent being **logically inapplicable**: consent presupposes an act one could refrain from performing, and nobody refrains from reflecting. Any architecture justifying sensing by a user's agreement is therefore void at the foundation - which matters, because it is the path the industry will take, and it will look reasonable all the way down.

There is a second failure, sharper than the first. **A reflection cannot be divided.** Two people in one beam produce one signal, and there is no way to separate your share of a room's echo from anyone else's. So in any space holding more than one person, one person's agreement becomes the instrument by which everyone else's protection is removed. The landlord agrees and the tenant is

measured. The employer agrees and the visitor is measured. One passenger agrees and the carriage is measured.

Consent, in this domain, is not a shield. It is a lever, and it is pointed at third parties.

What is actually being protected

Data protection law is built to permit processing once a lawful basis exists. File reflection there and nothing else, and the human body sits in a regime that legalises reading it whenever a box is ticked. But a reflection does not *describe* a body. It is the body, sampled. The distinction needed is not between sensitive and ordinary data but between data and **bodily integrity**, which is not negotiated and does not become permissible with paperwork.

To be exact, since the point invites misreading: this is a claim about what must be added, not about what can be escaped. Reflection-derived vital signs are personal data, and where they touch health they are the most strictly protected category there is. Nothing here argues for removing them from that protection - only that it is insufficient, because a person can consent to give up information and cannot meaningfully consent to being continuously readable.

The one gap the physics leaves

If reflection is unavoidable, is anything left to design? Yes, because the physics gives an instantaneous echo, and everything dangerous requires **accumulation**.

A single sample is a shapeless smear. To turn smears into an image, a gait, a breathing rate, the system must add up many samples with their phase aligned. And here a gap opens that is neither coincidence nor accident. Equalising a channel - what communication actually needs - is done inside the window in which the channel stays put, which at walking pace and a millimetre wavelength is under a tenth of a millisecond. Forming an image takes hundreds of milliseconds. Reading breathing and pulse takes seconds.

The same gap exists in space. Communication needs the nodes to agree on *time*, to within nanoseconds, and needs it badly. Coherent imaging needs them to agree on *phase*, which at 300 GHz means a fraction of a picosecond. Three orders of magnitude again, and again only one of them is necessary for the link.

Communication measures the environment as an obstacle. Surveillance measures it as an object. Different physical tasks that happen to begin with the same echo. From which the whole principle follows in one sentence:

Do not forbid the measurement. Remove the accumulation.

Take from the network what the link does not need and only observation requires - not as a policy, not as a setting, but as an absence in the construction. A policy of not collecting cannot be verified from outside. An absence stands a chance, being a property of the thing rather than of anyone's

conduct. A right to be forgotten should mean the memory does not exist, not that someone undertook to clear it.

The chance is not a certainty, and the difference is where the real work sits. Some absences announce themselves: whether a network maintains a common phase reference is measurable by anyone with a receiver. Others do not: no outsider can see how much memory a node has, and an absence that only a certifying body can attest to puts the construction back on somebody's word - the thing it was built to escape. Which absences can be demonstrated rather than certified is a question the accompanying technical work has to answer, and has not yet fully answered.

Privacy as a gradient, not a wall

The classical picture of privacy is a barrier: inside those who may know, outside those who may not, the boundary binary. A barrier either holds or is breached, which is why every breach is a catastrophe.

The physics of reflection proposes something stranger. Information about a body is not locked away at all. It radiates in every direction and fades with distance very fast, because the signal must travel out and back and so weakens twice over. Nobody is absolutely excluded. Everyone is at some distance, and distance is the measure of access.

A device against the body is a fraction of a metre from the surface it reads; a network node is metres away. That difference alone, before any question of permission, is an enormous advantage running in the person's favour by geometry rather than by anyone's decision. Nor is it escaped by splitting the network up: when transmitter and receiver sit apart, detectability is governed by the product of the two distances, and every arrangement of nodes is only a choice of where to draw those curves. A device carried on the body sits at the minimum of the product, both distances small at once. No geometry beats being there.

And motion the network must painstakingly estimate and subtract simply cancels for a device that moves with the body. What the person's device gets free, the network buys with power and precision.

> **A person is at zero distance from themselves. They are always the nearest observer of their own body. This is not a right that is granted. It follows from geometry, and the only thing a standard can do is avoid destroying it.**

Which gives a new definition of harm. The violation is not a leak. The violation is **flattening the gradient** - anything that erases the difference between how well a person can read themselves and how well the infrastructure can read them. Under this definition a network can be in breach while every policy is honoured and not one byte has escaped.

This is closer to how privacy has always worked between people than the barrier model ever was. We tell things to those who are close; closeness has always been the licence to know. Here that is not a metaphor about intimacy. It is the arithmetic of a radio link.

A correction to our own argument

Honesty requires a paragraph that weakens the series.

Parts One through Five argued that the network should have no owner: built from many small nodes, appearing wherever people appear, carrying connectivity to places a commercial operator will never serve. That argument stands, and the doctor in the regional town still needs it.

But the geometry cuts both ways. Because the echo weakens so steeply with distance, density is paid for in the margin that protects a person. Doubling the number of nodes per unit of area buys back about six decibels of that margin; doubling them along a street, where relays are actually strung, costs twice that. A dense, ownerless network of many nodes is, all else being equal, a better observer than a sparse network of a few operator masts.

We have spent seven articles arguing for the thing that makes surveillance easier.

The argument survives, but only under a condition we had not named. Density is safe only in a network built with the absences described above. Without them, decentralisation does not distribute power away from a centre. It distributes an eye across every street.

We would rather say this ourselves than have it said back to us.

Rescue without an observer

Here is the objection that destroys every privacy argument in this field, and it deserves to be met rather than deferred.

People do not carry their devices. Someone collapses in a bathroom with the phone charging next door. If protection means only your own device may read you, protection means nobody comes. The objection is correct and fatal to any scheme making safety conditional on participation: a protection available only to those who own the right hardware is a subscription to one's own body.

The way through is to notice that two different things are always requested under one word. *Something is wrong here* - one bit, now, in this room. And *who is here, where have they been, what were they doing* - identity, history, shape. They are demanded together because together they are irresistible, and permission granted for the first is always used for the second.

They sit in opposite corners of the physics, and the way through is to stop building a radar at all. Everything difficult about a watchman comes from making it active: a device that shines, listens for the echo, then has to be crippled so it does not hear too much. Invert it. Do not illuminate the person and read the reflection. Stay silent, and listen to what the person emits.

A body at thirty-three degrees radiates, and at these frequencies it radiates almost as a black body: the emissivity of human skin rises across this band towards 0.8, the emission formed in the outermost millimetre. The radiation passes through clothing, unlike infrared, so a blanket is no obstacle. Against a room at twenty degrees, a person is about ten kelvin warm.

A suitcase is not. Whatever it does not emit it reflects, and what it reflects is the same room, so its apparent temperature is the room's whatever it is made of. The contrast of a person is ten kelvin; the

contrast of a bag is zero. This is not a statistical separation a threshold has to be tuned into. It is structural.

And a receiver of this kind has nothing to be restricted. It transmits nothing, so there is no sounding signal to overhear. It has no phase, because thermal noise carries none. It has no aperture, so there is nothing to synthesise. It measures a temperature, not a rate, so a pulse is not a quantity it forms. The compromise one would otherwise be forced into - read the body a little in order to know that it is a body - disappears with the transmitter.

There is a further gain, and it answers the hardest question a standard faces. This absence is visible from outside. A device that does not transmit is audible by its silence; a device with no aperture is recognisable by its size. Turning a single-horn radiometer into a camera requires adding a lens and a focal-plane array - a change in the object, not a line in the firmware. It is an absence that can be demonstrated rather than certified.

What the device must be is best stated as what it lacks: one bit rather than a description, an absolute threshold rather than a personal one so it neither learns nor remembers who you are, no yesterday, and an alarm raised in the room rather than reported to a centre, with no way to raise it without the person present knowing. It knows that something the size and warmth of a person has not shifted for longer than a threshold. It does not know who.

And what cancels a false alarm is the part worth keeping. Not a password, not an account, not consent. **Movement.** A person with no device, no application and no registration silences it by being alive.

Two costs, and the first is a concession the earlier argument must make. **The gradient is shallower here.** A reflection travels out and back, which is what gives the person on the spot such an overwhelming advantage; thermal emission travels one way, so the same advantage is roughly halved in decibels. It is harder to hide from your own warmth than from your own echo, because in the first case you are the transmitter. The nearest observer is still you. The margin is simply smaller, and the argument should not pretend otherwise.

The second cost sets the design's real boundary. **Passivity alone guarantees nothing.** A calibrated radiometer with a narrow beam is a medical instrument: skin emissivity in this band tracks water content and thickness, differs measurably between men and women, and has been proposed for detecting eczema, burns and malignancy without contact. What makes the watchman safe is not that it listens rather than shines. It is one channel, a beam the width of a room, and no calibration reference - so that what it measures is the temperature of a space, not the condition of a skin. Those are the quantities a standard would fix, and anyone can check them from outside.

The rest belongs in the same breath. This works only where the network reaches. Radiators, laptops and cats are warm too, and the false alarm rate is a thing to be measured rather than calculated; in a room already at thirty degrees the contrast vanishes. Warmth is not life - a body cools over hours, so this says someone is there, not that they are still alive, and it will never separate deep sleep from unconsciousness. And access without the person's participation genuinely disappears: no authority can ask this network who is inside a building, because the network does not know. A standard built this way reduces the amount of compulsory access in the world. Pretending otherwise would cost more credibility than admitting it.

What a standard cannot reach

Everything above governs nodes that belong to a network and follow its rules. There is a receiver that does neither.

A device that transmits nothing and merely listens to traffic it did not initiate obeys no protocol, because it participates in none, and leaves no record, because transmitting is the only thing that leaves one. Nobody can be named as its operator, and a person who cannot know they were read will never complain. The parts cost tens of euros.

This must be conceded without softening, because it looks like it defeats the argument. It does not, for a reason worth stating precisely: a passive listener is limited to whatever the network radiates anyway, from wherever it stands, alone. It cannot summon the aperture, which requires nodes to cooperate, nor demand a sounding waveform, which requires the network to send one. Everything the architecture withholds from its own nodes it withholds from the eavesdropper too, because the eavesdropper's raw material is exactly what the network puts into the air.

So the division is this. The eavesdropper is a matter for law, and the law is already there: covertly reading a stranger's heart rate is not lawful anywhere in Europe, merely unenforceable. A standard governs the other thing, and it is the larger one. It decides whether ubiquitous, publicly funded, unavoidable infrastructure is a surveillance system by default. Turning surveillance from a free by-product of connectivity into a separate, deliberate, equipped act is the whole available prize - and the difference between what everyone can see for free and what someone must build on purpose is the difference between a society under observation and a society with some observers in it.

What this does to people

An architecture that touches every room deserves checking against what is known about people in rooms, and the findings are not uniformly kind to the proposal.

Being sensed is experienced as being watched, whatever the sensor. Studies of ambient monitoring in homes find residents describing detection and alerting as surveillance in so many words, reporting shame and the fear of judgement, and concluding that the safety gained does not justify the observation. Continuous monitoring produces anxiety and withdrawal even where everyone agrees it is protective. It would have been convenient to answer this by pointing at the smoke alarm in every bedroom, but the comparison does not hold: a smoke alarm watches the air, and anything that watches the room is understood, correctly, as watching the person in it. The absence of a camera resolves nothing. A radar that never sees a face is still felt as an eye.

The people most exposed are the least able to object. There is documented evidence that home sensing forms part of patterns of abuse against older people, and that residents with dementia end up in homes used *on* them rather than *by* them, unable to consent at all. This is not an edge case for the argument here. It is the argument, observed in the field: consent given by whoever holds the account, imposed on whoever occupies the room.

And the honest difficulty. The remedy proposed here puts the privileged observer on the person's own body. But surveys of older adults, their families and their nurses find ambient sensors preferred

to worn ones by a clear margin. Wearables are refused, forgotten, left charging. The people the rescue section is written about are the least likely to carry the device that protects them.

That last finding is not fatal, but it changes what can be claimed. Geometry gives the person tens of decibels over the network and gives them nothing at all if the device is in the next room. The privilege established here is a possibility rather than a protection: real, large, and contingent on a behaviour that cannot be assumed. A standard can preserve the gradient. It cannot make anyone stand in it.

Which names the one design consequence worth stating. If the advantage lives in proximity, the object carrying it must be one people already keep on them and do not experience as monitoring. That is a design problem, not a physics problem - and the sort that is solved badly when discovered late.

Why the objector benefits

The party expected to resist all this is the operator, on the grounds that a capability is an asset.

It is worth asking what kind. A network able to reconstruct the interiors of the buildings it serves must store that ability, secure it, defend it, and produce it on demand to every jurisdiction it operates in. It will be asked. It will be breached. It will be liable.

An operator structurally incapable of forming the image cannot be compelled to hand it over, cannot lose it, cannot be held responsible for it, and need not compete in a race for collection that the largest player wins anyway.

Incapacity, here, is a form of protection for the party deprived of it.

The closing

Faraday's candle cannot warm without shining. A 6G network cannot carry a message without measuring the room the message came from. That is settled, and no standard will unsettle it. What remains open is only this: who receives the picture.

There is a small symmetry worth noticing before the end. This whole argument is about the danger of being read by what bounces off you. The one thing in it that helps rather than threatens works the other way round: it does not read your reflection at all, it listens to what you emit. Nobody shines anything at you. You are not read. You are heard.

The series began with an ant that leaves a mark by choosing to leave it. It ends with a person who leaves a mark by existing. The ant's trace is an act. Yours is a consequence.

A network with no owner was the argument for taking power away from the centre. A reflection with an owner is the argument for giving something back to the person the centre never served: not a new right granted by a working group, but the oldest arrangement there is, which physics has already made and a standard can only preserve or spoil.

Nobody is closer to you than you.

Part of a series accompanying contributions to IEEE Industry Connections activity IC25-009-01, A Technical Reference Architecture Framework for an Open 6G Device Ecosystem. Part Seven addressed observation as a good that neighbours exchange by choice; this part addresses the person who exchanges nothing, agrees to nothing, and is measured anyway. The technical requirements following from these principles are the subject of a separate contribution.

Sources and prior work

Links marked *verified* were opened and read in full while preparing this article.

Physical figures. Chest wall displacement is from Z. Li, T. Jin, Y. Dai and Y. Song, *Through-Wall Multi-Subject Localization and Vital Signs Monitoring Using UWB MIMO Imaging Radar*, Remote Sensing 13(15):2905, 2021 - respiration 4 to 12 mm, heartbeat 0.2 to 0.5 mm: https://www.mdpi.com/2072-4292/13/15/2905 (open access, *verified*).

Thermal figures are from A. Y. Owda, N. Salmon, S. W. Harmer, S. Shylo, N. J. Bowring, N. D. Rezgui and M. Shah, *Millimeter-wave emissivity as a metric for the non-contact diagnosis of human skin conditions*, Bioelectromagnetics 38(7):559-569, 2017, doi:10.1002/bem.22074. That paper is the source of every thermal claim made here: emissivity rising from 0.4 to 0.8 across 30-300 GHz, emission formed within about one millimetre of the surface, water content dominating the electromagnetic behaviour of skin in this band, men measuring 0.046 higher than women, body regions differing by 0.06 to 0.08, a radiometer noise temperature of 453.7 K, and the proposal of the same measurement as a non-contact diagnostic for psoriasis, eczema, malignancy and burns. Open-access PDF: https://www.aaup.edu/sites/default/files/2021-10/bem.22074.pdf (*verified*).

Range resolution, wavelength, phase and the bistatic dependence on the product of two distances are elementary and can be checked in a line.

Standards. 3GPP TR 22.837, *Study on Integrated Sensing and Communication*, Release 19, version 19.4.0 of 28 June 2024: https://www.3gpp.org/DynaReport/22837.htm (*verified*; the document itself is at https://www.3gpp.org/ftp/Specs/archive/22_series/22.837/22837-j40.zip). ETSI's industry specification group on integrated sensing and communication published GR ISC 001 on use cases and GR ISC 002 on channel modelling in March 2025. In the WiFi domain, IEEE 802.11bf-2025 on WLAN sensing was published in September 2025.

Prior work on the privacy of channel-state sensing, which is older and deeper than a casual reader would assume. R. Lo Cigno, F. Gringoli, M. Cominelli and L. Ghiro, *Integrating CSI sensing in wireless networks: challenges to privacy and countermeasures*, IEEE Network 36(4):174-180, 2022, set out the core problem - that every receiver is already a sensor - four years before the present debate, together with countermeasures. See also *Addressing Privacy Concerns in Joint Communication and Sensing for 6G Networks: Challenges and Prospects*, arXiv:2405.01742, and *ISAC Privacy: Challenges and Solutions for 6G*, arXiv:2605.28325.

One recent publication should be named rather than left for a reader to find: Pascal Piron's account of the 802.11bf privacy debate, June 2026, https://pascalpiron.substack.com/p/wifi-sensing-and-the-privacy-fix (*verified*). It independently sets out two premises used here - that channel estimation is

mandatory and every receiver therefore already a sensor, and that the resulting standard offers nothing to non-participants - before going elsewhere, to what a working group did and did not resolve. The argument here is different in kind: that consent cannot be repaired because it does not apply, that what protects a person is a gradient rather than a barrier, and that rescue can be built on emission rather than reflection. The overlap in premises is real and acknowledged, and it is shared with the 2022 literature above.

Philosophy. That a person's relation to their own body is not a property relation, and privacy therefore belongs to human dignity rather than data ownership, is Luciano Floridi's; this article supplies a physical mechanism for something argued on other grounds.

Social findings come from the empirical literature on ambient monitoring in the home: qualitative work on privacy among older people and their carers, work on dignity in AI-assisted eldercare, design research on households with dementia documenting smart home technology within patterns of elder abuse, and twelve-month evaluations recording the preference for ambient over worn sensors.

Law. The footing for absence rather than promise is Article 25 of Regulation (EU) 2016/679, data protection by design and by default, which treats design-time architectural decisions as compliance choices and requires the most protective configuration as the default.