

The Network That Is Everywhere

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



Note on AI use: *AI tools were used in the preparation of this article, including research assistance and translation.*

6G links satellite and ground networks so a phone can reach help almost anywhere. The same reach lets the network sense people at home.

There is not a single tower on the mountain trail. The nearest base station stands in the valley, behind the ridge, and its signal does not reach this far. A hiker has twisted an ankle on the way down, the sun is setting, the temperature is dropping. He takes out his phone - an ordinary one, the same phone that lay on his desk in the city - and sends a message. The message goes through.

Not through a tower. Through a satellite that happens to be crossing the ridge at that minute. The phone does not know it has changed networks. The hiker knows even less.

This is what 6G can give people better than anything else. And if a few decisions are not made now, the same property will become its biggest problem. That is what this article is about.

A load test

Before a new bridge opens, it is loaded. Trucks full of sand are driven onto the span and parked in rows, the deflection is measured, engineers look for where a crack appears. A bridge is opened not when people believe in its strength, but when it is known where it bends and by how much.

The eight previous parts of this series built an argument: a network can have no owner, trust can live in a trace rather than in a vault, and a person remains the nearest observer of their own body unless the standard destroys that geometry. This part does something different. It puts the technology itself under load: it gathers everything that can be said against 6G, discards what does not survive a check against the facts, and looks at which solutions carry the weight and which break first.

Time for this is limited, and it has exact dates. Under the schedule 3GPP approved in June 2026, the requirements for the first release of 6G freeze in March 2027, the mechanisms in December 2028, the final text in March 2029. Whatever is not in the standard by those dates will be reproduced in equipment for twenty years.

What 6G really gives

Starting honestly means not starting with the weaknesses.

The biggest benefit of 6G for people is connectivity available almost everywhere. For the first time, ground and satellite networks are being designed as one system from the first release of the standard. In 5G, satellite connectivity arrived years after the first release, as an add-on. In 6G it is built into the studies from the start and aligned with the ground network from the beginning. For a person this means something simple: one phone, one network, and a path to connect even where there are no towers, or where a flood has destroyed them.

This is not a marketing promise but a stated goal. The International Telecommunication Union, in setting the framework for IMT-2030, named "connecting the unconnected", "ubiquitous connectivity" and "resilience" as overarching principles for every 6G scenario, and called low frequency bands key to nationwide coverage. Speed, holography, milliseconds of latency - all of that is in the standard too, but for most people it will change life little compared with 5G. Connectivity in the mountains, at sea, in a village, after a disaster changes it a great deal, because everyone at least once ends up where there is no signal, and that is exactly when it is needed most.

This benefit has three honest limits.

The first. About 300 million people live without mobile coverage today, roughly 4% of the world's population. Another 3.1 billion - 38% - live under coverage but do not use the internet. What holds them back is not a missing signal but the price of a device, awareness and skills: in low- and middle-income countries the cheapest smartphone costs about 16% of average monthly income, and for the poorest fifth of the population almost half. A network that is everywhere closes the first gap and does not close the second. A new generation with expensive devices may even widen the second.

The second. Satellite connectivity to an ordinary phone began in 5G. The contribution of 6G is not invention but integration into one system.

The third concerns failures. In November 2023 the core network of the Australian operator Optus failed. 2,145 people could not reach the emergency service, although other operators'

networks were working at the time. The response was not new technology but rules: the Australian government required that emergency calls in such an outage be carried by other networks. Resilience to the failure of a whole network is a matter of architecture and regulation. 6G can make it easier if it becomes a requirement of the standard. It will not arrive by itself with a new generation.

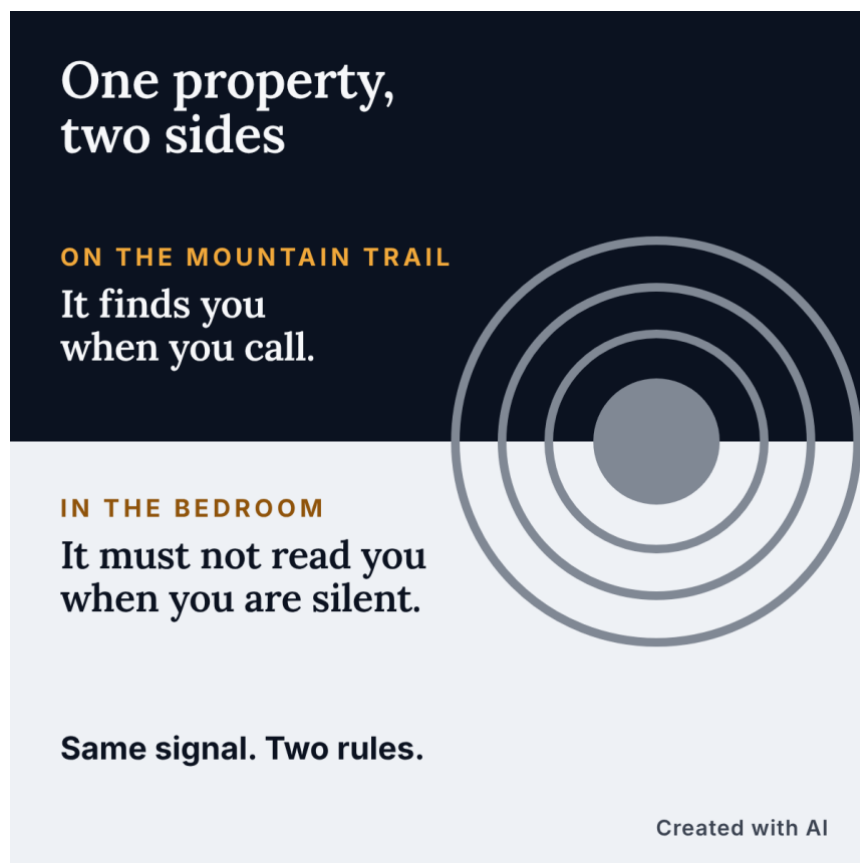
One property, two sides

Now let us go back to the mountain trail and look at the same scene from the other side.

A network that is everywhere also sees everywhere. Part Eight of this series explained why: to receive any message, a receiver must first measure the channel - how the signal was reflected, delayed and weakened on its way. At the bandwidths and frequencies of 6G, that measurement becomes a description of the space and of the people in it. It is not a feature somebody added. It is a condition of communication itself.

So the biggest benefit and the biggest risk of 6G are not two different things but one property seen from two sides. The connectivity that reaches the mountain trail also reaches the bedroom. A network that needs no separate sensor to find someone who is lost needs none to watch someone who never got lost.

Which side prevails is decided neither by physics nor by technology. It is decided by architecture, and architecture is being decided by the standard right now.



Where the bridge bends

If you gather everything that can be said against 6G and discard what does not survive scrutiny, little remains, but what remains is heavy.

The network sees people. This was said above and in detail in Part Eight. I will add only what emerged under load: the danger is smaller than in the frightening forecasts and greater than in the reassuring ones. For images and outlines, the network needs many nodes to work as one antenna. Breathing needs far less: more than ten years ago it was shown that a person's breathing can be detected from signal strength alone across many ordinary wireless links in about half a minute, with an error of about a third of a breath per minute. No phase of any kind is required.

The network speaks about those who stay silent. Devices that exchange observations about the world inevitably say something about people who bought nothing and agreed to nothing. A 2025 study showed that from the service information Wi-Fi devices transmit in the clear, a walking person can be recognised among previously recorded people with 99.5% accuracy.

The network gathers power. Whoever holds the network's memory, trust and decisions becomes a centre that can be compelled, breached or switched off. And a centre forms easily: manufacturers already describe sensing as a new source of revenue and name security and government as the first customers.

The network decides for itself. Built-in AI is faster than a human, but it can be deceived, its decisions are opaque, and an error in one node can cascade through the whole network.

The network outlives its cryptography. 6G will operate from around 2030 to 2050 - exactly when data intercepted today may begin to be decrypted by a quantum computer. This hits hardest not the encryption of the radio link but what keys, signatures and anonymity rest on.

The network eats its own gains. The energy needed to send one bit falls with every generation, while the total consumption of networks grows, because traffic grows faster.

The network needs density and pays for it. A connected network without an owner appears abruptly, once a device has on average more than four or five neighbours. But every doubling of node density eats into the margin that protects a person from being read.

The network is not for everyone. If a base station is unprofitable, it will not appear, however many protocols surround it. Whoever lives outside the commercially viable zone risks getting nothing once again.

The network goes where knowledge is thin. Below 300 GHz there is plenty of data, and major reviews have found no proven harm. Above it, in the sub-terahertz range, data is scarce, and the International Commission on Non-Ionizing Radiation Protection itself acknowledges a gap at that boundary. The new bands also sit next to radio astronomy and satellites.

The solutions that break first

Under load, the first to break are not the bad solutions but the obvious ones.

Consent. All of data protection rests on the assumption that data comes from a person who could choose not to send it. A reflection is created by the receiver. Nobody can decline to reflect, so consent is logically inapplicable here, and in a room with several people one person's consent removes the protection of the others.

The off switch. A switched-off sensing function protects against the operator, but not against an outsider: the communication signal remains an illuminator for any foreign receiver. Calculations for the proposed 6G bands showed that they suit passive radar even better than earlier sources.

Coarsening. Making observations about the world coarser is nearly useless: halving the resolution makes it only 6-9% harder to single a person out. Publishing less often is useless too if every statement is rich: recognition arrives within a few dozen such statements.

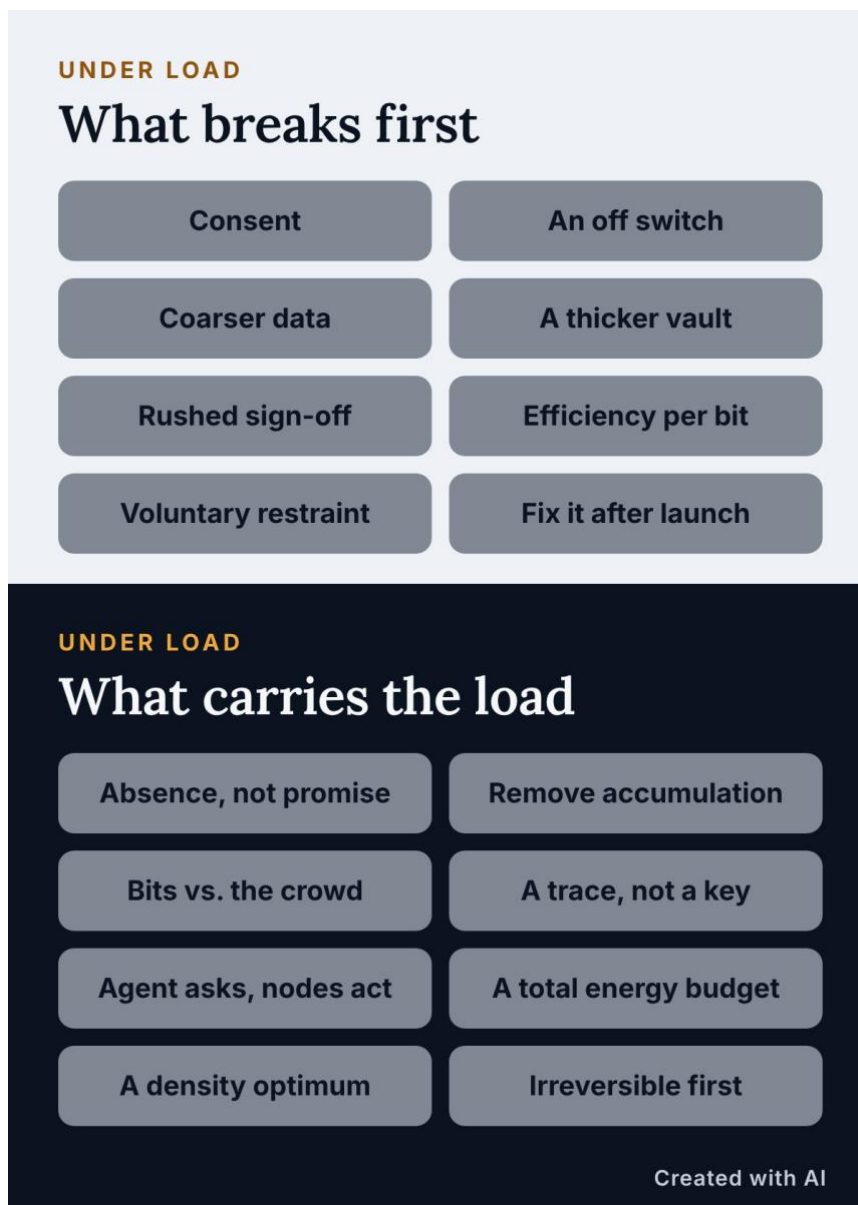
A thicker door. A more secure vault answers the question "how do we make a break-in harder". It loses on the day the break-in happens anyway, because everything behind the door is kept in one place.

A human in the loop with a stopwatch. Under pressure and in a hurry, people start approving automated decisions without looking. A systematic review of 74 studies names time pressure as a factor that strengthens this trust. A human with a stopwatch turns into a rubber stamp.

Efficiency per bit. If energy use is capped per gigabyte, traffic growth meets the cap on its own: the share of fixed power is diluted, the per-unit figure falls, and total consumption rises. Such a cap rewards exactly what it was meant to prevent.

Voluntary restraint. It pays an operator not to be able to see: such an operator cannot be compelled, breached or held liable. That is true for all operators together. For each one individually, selling sensing pays better if the others abstain. It is a classic prisoner's dilemma, and one party's voluntary restraint does not hold in it.

"We will fix it after launch." Only what has not gone into hardware and protocols can be fixed.



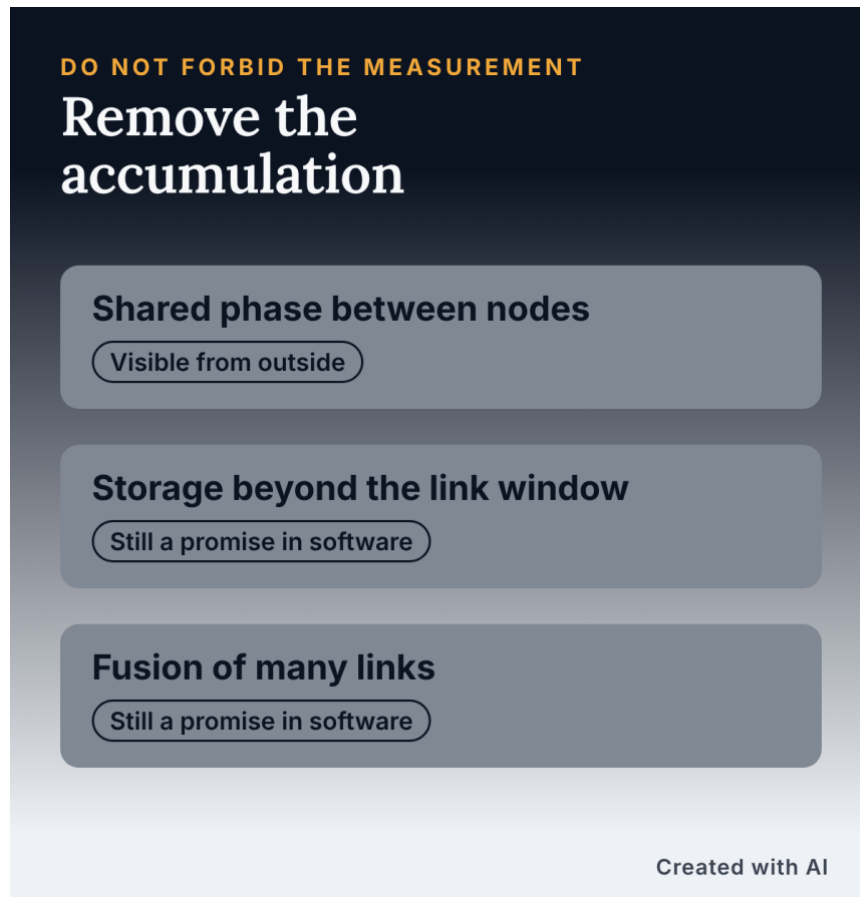
What carries the load

What holds up is built differently. It does not promise good behaviour. It makes bad behaviour impossible by design, useless when attacked and visible from outside.

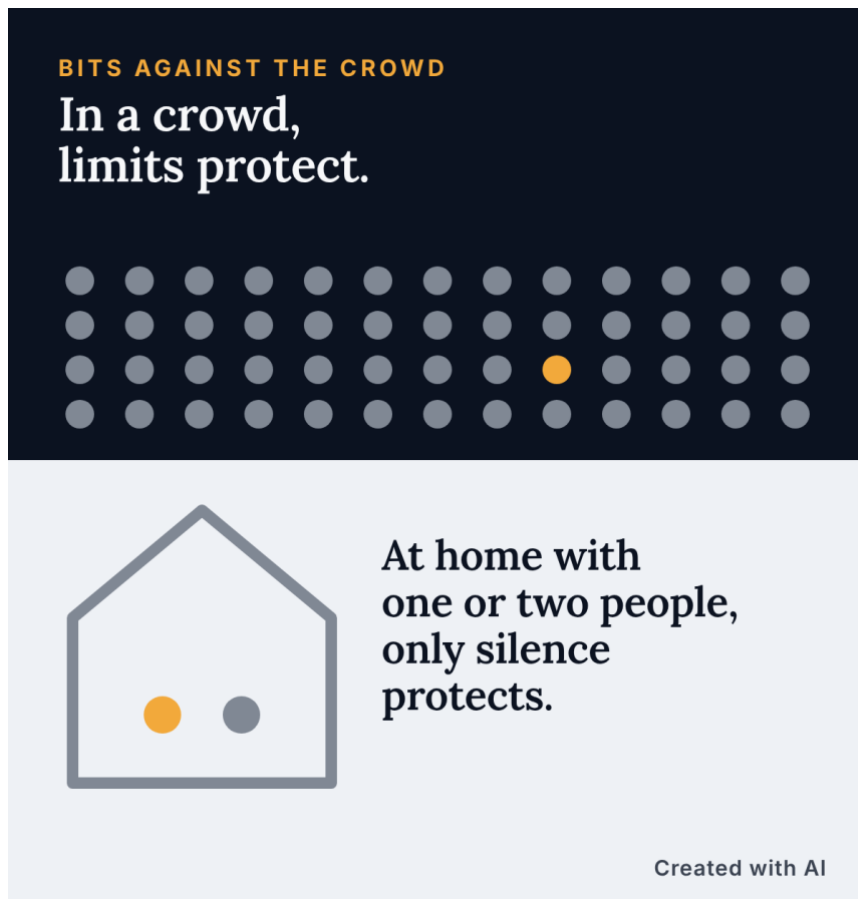
Absence instead of a promise. A promise of "we won't" cannot be verified from outside. The absence of a capability sometimes can. Part Eight put it in one sentence: do not forbid the measurement, remove the accumulation. A single instantaneous reflection is a shapeless blur. Images, gait and breathing come only from accumulating many measurements. Communication does not need that accumulation; observation cannot do without it.

The load test clarified what exactly has to be removed. Not one thing, but three. A shared phase between nodes - without it there are no images and no outlines. Storage of measurements beyond the window that communication needs. And the fusion of measurements from many links - which is what makes breathing visible from signal strength alone. The first can be seen

from outside: any receiver can measure a shared phase reference. The second and third remain, for now, promises written into device software. That is an honest limit of the solution, and it should be named.



Bits against the crowd. Protecting observations has a simple measure. To single out one person among everyone on Earth takes 34 bits of information: $\log_2$ of 9 billion, rounded up. The count uses 9 billion rather than today's 8.3 because the population will reach that mark while the standard is in service, and 33 bits will then no longer be enough. Among the residents of a building of a thousand people, about 10. Within a family of four, two bits. Protection works as long as noticeably fewer bits leak in a period than are needed to single a person out of their surroundings. Hence the order proposed in the specification that accompanies Part Seven: first decide what may be talked about at all (a place - yes, a person - no), then limit how much a single statement may contain, and only then how many statements may be sent. In a crowd, the limit protects. In a flat with one or two people, only silence protects. And because bits add up over time, a limit needs not only a size but also a lifetime.



A trace instead of a key. A lock should have no single key. Trust is spread across several foundations that share no common weakness, and everything else - commissions, permissions, path tags - lives as a trace with a limited lifetime. The goal changes: not to make compromise impossible, but to make it useless and visible.

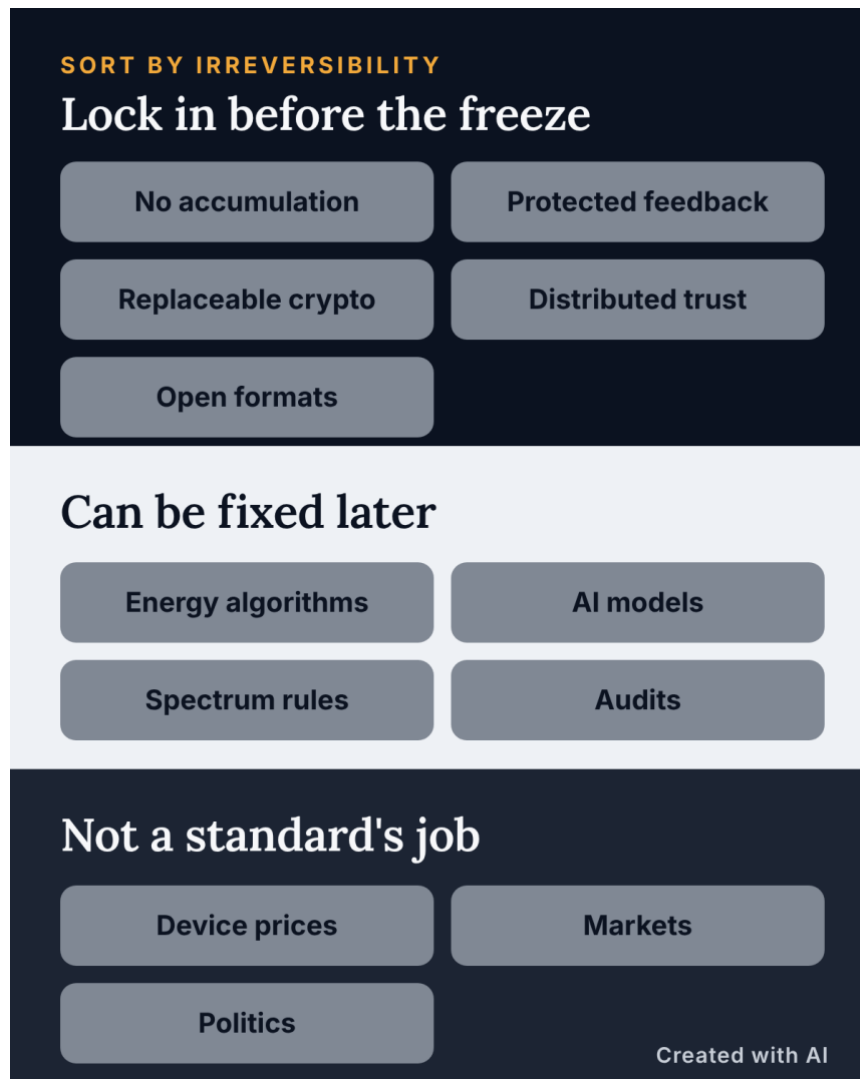
The agent asks, the environment acts. An AI agent receives not a key but a commission with narrow limits and an expiry. It can only propose an action, and independent nodes carry it out, each checking for itself whether the action fits the limits. A human is needed where an action is irreversible - with personal accountability, not a stopwatch. This scheme has two weak points, and they should be named too. Each action may fit the limits while their sum does not, so the accumulated result must be checked as well. And power passes to whoever writes the rules for commissions, so this new centre must also be visible and accountable.

Replaceability instead of replacement. The quantum threat is not solved by replacing algorithms once: they will change again. Replaceability must be a property of the architecture, built in before launch, while old choices have not yet become sunk costs.

A budget instead of efficiency. What should be capped is total consumption for an agreed task - coverage, capacity - taking into account fixed power and the whole life cycle of the equipment. The per-gigabyte figure is worth publishing, but not worth targeting.

An optimum instead of growth. Network density has a lower bound, below which there is no network, and an upper one, above which the network becomes the best observer. The first device must be useful to its owner on its own, otherwise nobody buys it and the network never starts.

Sorting by irreversibility. What will go into hardware and protocols for twenty years - the absence of accumulation, protection of channel feedback, replaceable cryptography, distributed trust, open formats - must be locked in before the freeze: requirements for outcomes by March 2027, mechanisms by December 2028. What can be changed by software or regulation can be left for later. Markets and politics are not solved by a standard, and saying so honestly is also part of the solution.



And one condition above all the others: mandatory, not recommended. Inconvenient proposals are rarely rejected openly. They are accepted by name and emptied of content - made optional, given broader exceptions, postponed to the next release.

Corrections to our own series

Since Part Eight, this series has kept a rule: better to say the inconvenient thing ourselves than to hear it said back to us. The load test produced several such corrections.

Incapacity benefits the operator only together with everyone else. Part Eight argued that giving up the ability to see protects the operator itself. That is true, but only as a shared

commitment that cannot be quietly withdrawn. There is also a player the series did not name: the state. For the state, a network's inability to see is not a protection but a loss. A realistic coalition for such a commitment includes data protection regulators, consumer organisations, operators who fear liability, and the research community. Sellers of sensing services and parts of the security establishment will be on the other side. This is worth knowing in advance.

Accumulation is not only phase. Early architectural sketches in this series relied on coherent relaying: neighbouring nodes preserve the phase of the signal and work as one distributed antenna synchronised by atomic clocks. That brings a gain in communication. And it is exactly the interferometer Part Eight proposed to remove. The contradiction will have to be resolved, for example by keeping phase coherence within a single node and coordinating between nodes only in time. How much communication gain that costs must be calculated, not assumed.

The factory setting is a strong lever, but not an all-powerful one. Part Seven argued that the decision belongs not to the owner but to the default. The evidence supports this: a synthesis of 58 studies shows a strong influence of defaults on choice. But choice and outcome are different things. Participation by default holds as long as its costs are small and unnoticed. A noticeable loss, such as battery, will make people switch it off.

A network where people are is not about all of the unconnected. Parts Three and Five spoke of the person outside the commercially viable zone. The argument is sound, but it applies to a minority of the unconnected. Most of them already live under coverage, and what stops them is the price of a device. So the series must add a reverse requirement: 6G must not worsen the position of those who stay on devices from earlier generations.

The trust core is not yet ready for the quantum future. The anonymous attestation on which device indistinguishability and the checking of agents' commissions rest is today standardised only in classical cryptography. Post-quantum schemes exist in research, not in standards. And a post-quantum signature is dozens of times longer than today's: 2,420 bytes against 64, while the path tag proposed in Part Four itself takes 16 bytes. Signing every tag separately will become impossible, and the way of signing must be defined now.

Where the logic does not yet close

An honest conclusion must also name the places where the solutions pull in different directions.

A distributed network wants many nodes to work as one antenna. Protecting people wants them unable to do so. A network without an owner needs density, and density eats the privacy margin. Open formats remove the manufacturer's power and open the door to attack if their protection is optional. Remove the centre from data transport and it easily reappears one level up - in the assembly of knowledge, in certification, in the rules for commissions. And the advantage of proximity on which all of Part Eight rests works only if the device is on the person, while devices are often taken off, forgotten, left on the charger - most often by exactly those for whom all of this is intended.

These contradictions do not refute the logic of the solution. They show where it requires a choice, not only a principle.

What the test showed

The bridge held not where it was reinforced with promises, but where the absence of the part needed for abuse was built into the structure. It bent where a solution relied on goodwill - of the operator, of the state, of a human with a stopwatch, of a device owner who will one day begrudge the battery.

Technically, almost everything described here is possible. That is not the question. The question is who will ask three simple questions in the room where the standard is written, while there is still time before March 2027. What will a person outside the commercially viable zone get from 6G - not on average, but they themselves? Who has the right to set the default? And which absences of capability will be fixed in the standard as mandatory, and which will remain words?

The hiker on the mountain trail will receive a reply to his message. Rescuers will find him by the coordinates his phone sent along with the text. That is the best thing 6G can do, and it is worth building for that alone.

But the same network that found him on the trail will also stand in his home, in the bedroom, where he needs no one. Finding a person when they ask, and not reading them when they are silent, are not two different technologies. They are one network with two rules. Physics has already fulfilled the first. Only the standard can fulfil the second.

A network that is everywhere must know how not to be where it was not invited.

Parts One through Six argued for a network with no owner, Part Seven stated the condition under which such a network can begin, Part Eight addressed the person who is measured without taking part. This part puts the whole construction to a load test: what 6G gives, what it costs, and which solutions carry the weight.

Sources and prior work

Standard timeline. 3GPP, Release 21 timeline approved at TSG#112 on 10 June 2026:
<https://www.3gpp.org/news-events/3gpp-news/rel21-timeline>

6G objectives. ITU-R WP 5D, IMT-2030 Framework, common slide deck, February 2024:
[https://itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2030/Documents/2024-February_Common%20slide%20deck%20\(IMT-2030%20Framework\).pdf](https://itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2030/Documents/2024-February_Common%20slide%20deck%20(IMT-2030%20Framework).pdf). Primary document: Recommendation ITU-R M.2160-0 (11/2023), via the link in Part Seven:
https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2160-0-202311-I!!PDF-E.pdf

Satellite connectivity in 6G. Samsung Research, "NTN and TN networks for the 6G era: technology overview and regulatory challenges": <https://research.samsung.com/blog/NTN-and-TN-networks-for-the-6G-era-technology-overview-and-regulatory-challenges>

Coverage gap and usage gap. GSMA, State of Mobile Internet Connectivity, 2024 data: <https://gsma.com/newsroom/press-release/gsma-calls-for-renewed-focus-on-closing-the-usage-gap-as-more-than-3-billion-people-remain-offline-despite-available-mobile-internet-services/>. ITU, Facts and Figures 2025: <https://www.itu.int/hub/?p=47779>

The Optus outage. ACMA, announcement of the Optus penalty for the emergency call outage, November 2024: <https://www.acma.gov.au/articles/2024-11/optus-pays-12-million-penalty-triple-zero-outage>.

Australian Government response to the review of the 8 November 2023 outage:

https://www.infrastructure.gov.au/sites/default/files/documents/review_into_the_optus_outage_of_8_november_government_response.pdf

Breathing from signal strength. N. Patwari, J. Wilson, S. Ananthanarayanan, S. K. Kasera, D. R. Westenskow, "Monitoring Breathing via Signal Strength in Wireless Networks", IEEE Transactions on Mobile Computing; preprint: <https://arxiv.org/abs/1109.3898>

Recognition from Wi-Fi service information. J. Todt, F. Morsbach, T. Strufe, "BFId: Identity Inference Attacks Utilizing Beamforming Feedback Information", ACM CCS 2025, DOI 10.1145/3719027.3765062: <https://publikationen.bibliothek.kit.edu/1000185756> (via the sources of Parts Seven and Eight)

The weakness of coarsening. Y.-A. de Montjoye et al., "Unique in the Crowd: The privacy bounds of human mobility", Scientific Reports 3, 1376, 2013: <https://www.nature.com/articles/srep01376>

Passive radar at 6G frequencies. "Feasibility of Adopting 6G Frequencies for Transmitter of Opportunity by Passive Radar", IEEE iSES 2022: <https://idr.nitk.ac.in/items/4df8329e-54f4-4f0b-8dba-53cb4105b7f4/full>

Sensing as a revenue source. Samsung Research, "Integrated Sensing and Communication (ISAC): New monetization opportunities for 5G and beyond": <https://research.samsung.com/blog/Integrated-Sensing-and-Communication-ISAC-New-monetization-opportunities-for-5G-and-beyond>

Automation bias. K. Goddard, A. Roudsari, J. C. Wyatt, "Automation bias: a systematic review of frequency, effect mediators, and mitigators", JAMIA 19(1), 2012: <https://academic.oup.com/jamia/article/19/1/121/732254>

Efficiency and consumption. S. Tombaz, K. W. Sung, J. Zander, IEEE Wireless Communications Letters, 2014: https://people.kth.se/~sungkw/files/tombaz_sung_zander_wcl_2014.pdf

Defaults. J. M. Jachimowicz et al., "When and why defaults influence decisions: a meta-analysis of default effects", Behavioural Public Policy, 2019: <https://collaborate.princeton.edu/en/publications/when-and-why-defaults-influence-decisions-a-meta-analysis-of-defa/>. Kalkstein et al., "Defaults are not a panacea", Behavioural Public Policy 9, 2025: <https://www.cambridge.org/core/services/aop-cambridge-core/content/view/A9CDEBE021D23C750E14F58C03D2DD83/S2398063X22000240a.pdf/defaults-are-not-a-panacea-distinguishing-between-default-effects-on-choices-and-on-outcomes.pdf>

Exposure above 300 GHz. ICNIRP, Annual Report 2025: https://www.icnirp.org/cms/upload/doc/Annual_Report2025.pdf

The quantum threat and standards. 3GPP SA3, transition to post-quantum cryptography: <https://www.3gpp.org/technologies/pqc-sa3>. Post-quantum anonymous attestation: EU project FutureTPM: <https://www.cordis.europa.eu/project/id/779391/reporting/fr>. ML-DSA signature sizes per FIPS 204: <https://www.ietf.org/archive/id/draft-sfluhrer-ssh-mldsa-04.html>

Prior work close in spirit. The view that coverage and seamless connectivity matter more to people than speed is argued independently by New America, "What 6G Should Be: Ubiquitous and Seamless Connectivity, Not Just Another 'G'": <https://www.newamerica.org/insights/what-6g-should-be/>. The case for building privacy into ISAC from the start, rather than adding it later, is made by the Barkhausen Institut, "When 6G becomes a sensor": <https://www.barkhauseninstitut.org/en/press-release-when-6g-becomes-a-sensor>. The argument here differs in treating benefit and risk as one property and in its choice of remedies.