

WiFi - What It Can See In Your Home Or Business

The field of wireless technology has fundamentally evolved beyond simple internet communication into a medium for **spatial intelligence**. If you are positioning **hardwired Ethernet installations** as the premium choice for security, privacy, and performance, you have incredible, scientifically backed arguments at your disposal. [1]

Modern Wi-Fi routers can now function as a camera-less, device-free surveillance grid. They achieve this by utilizing the existing radio frequency (RF) environment to map physical spaces, track human movement through walls, and read biological metrics—all without requiring a person to carry a smartphone or wear a smartwatch. [1, 2]

1. Wi-Fi Sensing & The 802.11bf Standard

The wireless industry officially ratified **IEEE 802.11bf**, the dedicated global standard for Wi-Fi sensing. [1, 2]

The Concept: Think of a Wi-Fi router less like a data pipe and more like an active submarine sonar.

How it works: Because the human body is mostly water, it absorbs and scatters microwave frequencies. Devices constantly measure **Channel State Information (CSI)**—microscopic changes in how radio waves bounce and return to optimize connection.

The Surveillance Shift: AI models decode this CSI data stream to turn standard internet hardware into a 3D radar system. [1, 2, 3, 4]

2. What Wi-Fi Can "See" Right Now

WiFi - What It Can See In Your Home Or Business

A building equipped with modern Wi-Fi routers (running automated, over-the-air firmware updates from ISPs) can track the following metrics without your permission: [1, 2, 3]

Near-100% Individual Identification: Researchers at the Karlsruher Institut für Technologie (KIT) proved that standard, unmodified Wi-Fi routers can extract unencrypted "beamforming feedback information" to identify an individual with near 100% accuracy within seconds. By mapping how a person blocks signals, the AI creates a biometric signature of their specific posture, weight shift, and gait (how they walk). It recognizes *who* you are even if you turn your phone off. [1, 2, 3, 4]

3D Pose Reconstruction through Walls: Systems like the open-source *RuView* project use AI to track the exact real-time 3D posture (head, torso, limbs) of human figures hidden behind solid drywall and doors. [1, 2, 3]

Medical-Grade Heart Rate & Respiration Tracking: Systems like *Pulse-Fi* (developed by UC Santa Cruz) can isolate microscopic, millimeter-level Doppler shifts caused by human biology. They filter out ambient room noise to detect chest expansions and heartbeats from feet away with a clinical accuracy of 96.8% — entirely contact-free. [1, 2, 3, 4]

Keystroke and Emotion Detection: Machine learning algorithms can parse dense Wi-Fi ripples to map tiny finger movements on a table (effectively reading typing patterns) or flag emotional spikes based on sudden shifts in respiration and micro-movements. [1, 2]

The Privacy Loophole: Why This Sells Ethernet

WiFi - What It Can See In Your Home Or Business

This technology creates a severe, unprecedented threat to physical privacy that is highly effective for an Ethernet installation pitch:

Invisible & Passive: Unlike smart cameras or smart microphones, there is no physical lens to cover, and you don't have to opt into a wearable tracker. The surveillance occurs passively through waves already flooding the home.

Completely Unencrypted Signals: The underlying mechanism that researchers use to bypass security is **Beamforming Feedback Information (BFI)**. Devices send these mapping reports completely unencrypted so routers can direct signals toward them. Anyone with a cheap, modified Wi-Fi card nearby can passively intercept this data to track movements inside a home or business.

Legal Gray Area: Current wiretapping and privacy surveillance laws are strictly structured around optical video recording and acoustic wiretapping. They completely fail to cover ambient radio wave spatial harvesting. [1, 2, 3, 4, 5]

Your Pitch to Clients

"Radio waves cannot be blocked without destroying your wireless connectivity. If you want absolute physical privacy, zero passive tracking from neighboring networks or ISPs, and a system impervious to wireless hacking, you must take the data out of the air. Hardwired, shielded Cat6 Ethernet is the only way to lock down your home or office environment." [1]

WiFi - What It Can See In Your Home Or Business