AUDEAMUS GROUP, LLC

Wi-Fi Sensing & Privacy Weekly Brief

October 30, 2026 | Research published October 23-30, 2026

THIS WEEK'S JUDGMENT

Two research reports put sensing inference closer to the radio and improve passive tracking methods. IEEE privacy work and proposed consumer IoT labeling rules also advance. None establishes broad household deployment or complete consumer control over derived presence and activity inferences.

01 / PREPRINT / FPGA HARDWARE PROTOTYPE / 2026-10-27

Activity classification runs inside the radio

Key finding. A 132-neuron spiking classifier on an RFSoC reports 94.7% activity accuracy, 90.7% macro-F1 and 206-microsecond inference on IEEE 802.11ay micro-Doppler data. It outputs an activity label from programmable logic.

Why it matters for Audeamus. Local inference could reduce raw-signal transport and support an always-on sensing path. Ask what remains powered and what labels leave the device.

Evidence limits. Four activities and seven people do not establish household performance. Test-subject tuning makes accuracy optimistic by about 1.5 points. Dynamic-energy comparisons exclude the receiver and spectrogram front end; static FPGA power dominates.

Read in full? Read the hardware measurements and explicit accuracy and energy omissions.

Open original source

02 / PREPRINT / SINGLE-OFFICE EXPERIMENT / 2026-10-25

Passive CSI tracking learns changing uncertainty

Key finding. A physics-informed state-space model learns uncertainty in angle, delay and Doppler observations without position labels. Its WiDFS-based evaluation reports 0.67-meter mean absolute tracking error, 31.9% lower than raw WiDFS.

Why it matters for Audeamus. Label-free training could reduce calibration work if the method transfers to unfamiliar rooms and residents. That transfer needs its own test.

Evidence limits. The paper evaluates a walking target in one office on Intel 5300 hardware. Participant and independent-trajectory counts are not stated, and unfamiliar homes and quiet presence are untested.

Read in full? Skim the uncertainty model and inspect the single-setting evaluation.

Open original source

© 2026 Audeamus Group, LLC. All rights reserved. This report is the property of Audeamus Group, LLC and reflects solely its opinions. It is for informational purposes only and must not be relied upon as legal or investment advice. Third-party materials remain the property of their respective owners.

Wi-Fi Sensing & Privacy Weekly Brief

October 30, 2026 | Research published October 23-30, 2026

03 / PUBLISHED IEEE STANDARD / PUBLIC STATUS RECORD / 2026-10-23

IEEE 802.11bi-2026 is an active privacy amendment

Key finding. IEEE lists 802.11bi-2026 as an active standard, published October 23 after September 25 Board approval. It modifies the Wi-Fi MAC sublayer to enhance user privacy.

Why it matters for Audeamus. Ask vendors which privacy mechanisms they implement and how users control sensing-derived inferences.

Evidence limits. The public record is not the normative text, which requires purchase or subscription. Publication alone proves neither vendor adoption nor household sensing controls.

Read in full? Have the product team review the exact specification before claiming compliance.

Open original source

04 / FCC PUBLIC NOTICE / PROPOSALS, NOT FINAL RULES / 2026-10-27

Cyber Trust Mark operating proposals invite comment

Key finding. The FCC's October 27 record identifies a request for comment on Cyber Trust Mark label design and surveillance. The public sensing summary reports proposals for renewal, post-market oversight and sensor-capability disclosures.

Why it matters for Audeamus. Track the consultation when planning consumer sensing products. Cybersecurity labeling and consent to derived RF inferences are separate questions.

Evidence limits. These are proposals, not adopted requirements. The full notice returned an access error in this review, so its detailed provisions remain reported rather than independently checked.

Read in full? Read the original notice when accessible before relying on a proposed obligation.

Open original source

ONE QUESTION TO TAKE TO A VENDOR

Ask what the product infers about people, where those inferences are computed, who can disable the sensing function and how derived records are retained or deleted. Treat a local activity label and a cybersecurity mark as evidence to examine, not as proof of household consent.

This edition uses only the October 30 public Wi-Fi Sensing Review summary and cited original sources. No private desk analysis is reproduced. IEEE status is verified from its public record. FCC notice details remain qualified because the full notice could not be retrieved in this review. Implications are Audeamus analysis, not legal advice.

Read the original public sensing summary

© 2026 Audeamus Group, LLC. All rights reserved. This report is the property of Audeamus Group, LLC and reflects solely its opinions. It is for informational purposes only and must not be relied upon as legal or investment advice. Third-party materials remain the property of their respective owners.