AUDEAMUS GROUP, LLC

Wi-Fi Sensing & Privacy Weekly Brief

September 25, 2026 | Historical public-summary edition

HISTORICAL PUBLIC SUMMARY

Wi-Fi sensing meets multi-occupant scale — and an RF-layer privacy defense

September 18–25, 2026 · Three new preprints met the relevance, date and evidence checks. New research: a remote zero-knowledge defense against unauthorized Wi-Fi activity recognition, a multi-user CSI model revised this week, and a 5G CSI augmentation method. Meaningful standards and regulatory updates: none verified for inclusion. The strongest signal is a shift from proving that RF sensing works to handling mixed occupants, scarce training data and active resistance; none of the studies yet demonstrates a consumer-ready product or standardized privacy control.

01 / NEW · arXiv preprint · Kim et al. / 2026-09-21

Zero-Knowledge Remote Adversarial Attack against Wi-Fi-based Human Activity Recognition for Privacy Protection

Key finding. Introduces GRAW, a router-side privacy defense that perturbs Wi-Fi signals used by an unauthorized receiver to estimate CSI. A generative-adversarial imitation-learning policy is designed to work without knowledge of the target model or its inputs, and the authors report real-time over-the-air software-defined-radio tests.

Why it matters for Audeamus. This is a rare control aimed at the sensing channel itself rather than at a vendor's app or stored data. Across seven tested HAR models and five environments, the authors report degradation to random-selection performance while preserving more than 99% ordinary packet success, suggesting a path to privacy protection that can travel with the transmitter.

Evidence limits. It is an unreviewed preprint demonstrated with software-defined radios, not a commodity-router feature. Active perturbation raises coexistence, regulatory, and ownership questions; the evaluation covers activity recognition, not every presence or localization method, and the headline 76.7% advantage is relative to selected attack baselines at the same perturbation level.

Read in full? Read in full. It reframes consumer control as a physical-layer capability and supplies the week's most consequential evidence, but implementation and policy constraints are central to the result.

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

September 25, 2026 | Historical public-summary edition

02 / NEW · arXiv preprint, revised v2 · Yuan et al. / 2026-09-21

WiFi-based Multi-user Activity Recognition via User-Conditioned Spatial Attention

Key finding. The paper adds user-conditioned spatial attention: learnable user-slot embeddings modulate separate attention maps before classification instead of trying to separate all users only at the output. On the WiMANS benchmark, the model reports more than 93% average accuracy with five concurrent users across three rooms and outperforms nine baselines.

Why it matters for Audeamus. Multi-occupant interference is a core barrier to in-home sensing. Associating overlapping CSI patterns with per-user outputs in one model could support richer household services without instrumenting each person, and the gap over the strongest baseline grows to roughly three to four points with four or five users.

Evidence limits. The random 9:1 split reuses a single benchmark with only five participants, five fixed locations and three controlled environments; it does not test unfamiliar homes or people. The learned IDs are dataset user slots, not a demonstrated real-world identity-assignment mechanism, and deployment must also handle changing occupants and arrivals.

Read in full? Read in full. The architecture attacks a commercially important failure mode, while the split design and user-slot assumption need close reading before accepting the accuracy claim.

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

September 25, 2026 | Historical public-summary edition

03 / NEW · arXiv preprint · Li et al. / 2026-09-24

Structured Pose-Conditioned Flow Matching for Generative 5G CSI Augmentation

Key finding. The paper proposes StructFlow-HPR, which learns a pose-conditioned flow in a topology-preserving latent space to generate synthetic 5G CSI–pose pairs. On one real prototype dataset, adding generated samples raises overall PCK@5 from 72.43% to 73.71%, with larger gains for the most difficult lower-leg action.

Why it matters for Audeamus. Synchronized RF-and-pose collection is expensive, so useful synthetic CSI could cut the data cost of ambient sensing and speed adaptation to new actions. The work also shows that the data-scarcity problem is moving beyond Wi-Fi into broader integrated communication-and-sensing platforms.

Evidence limits. This is 5G sensing, not Wi-Fi, and the prototype uses one phone, three fixed remote radio units and a 3.3-by-2.7-meter area. The overall strict-threshold gain is only 1.28 percentage points; cross-room and multi-person tests are left for future work, and t-SNE overlap is weak evidence of physical realism.

Read in full? Skim. The augmentation idea is relevant to RF-sensing economics, but the small single-setting gain and adjacent 5G scope do not justify a full read for Wi-Fi specialists.

Open original source

ARCHIVE NOTE

This edition preserves the dated public summary and original citations from Wi-Fi Sensing Review. It has been repackaged for the Audeamus Group archive; the historical claims have not been independently reverified during this formatting pass. No private desk analysis is included.

Original public Wi-Fi Sensing Review

© 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.