

Towards Secure and Trustworthy Human-Centered Wireless Sensing

By Tanvir Ahmed (Cornell Tech)

Towards Secure and Trustworthy Human-Centered Wireless Sensing

By Tanvir Ahmed (Cornell Tech)

Today, we are surrounded by many wireless signals such as radio, cellular, or Wi-Fi in almost every environment. Without even realizing it, we are physically interacting with these signals all the time. When we move, speak, or just exist in such an environment, the surrounding signals and their reflections can be analyzed to reveal a lot of information about ourselves. That is the essence of wireless sensing: think about the standard presence sensor in your room, or a Google Nest Hub tracking sleep and breathing wirelessly from the bedside table [1].

Products built on this technology are already widely deployed. Apps/devices like SleepScore [2], Pronto Sense [3], and Logitech Spot [4] have a real impact on quality of life, especially for elderly care and people who are unable or do not prefer wearable devices. Because they capture less recognizable visual information than camera-based systems, they are widely marketed as "privacy-preserving" alternatives [5].

However, this privacy by modality is only part of the story. Even without capturing recognizable visual information, the continuous data stream from wireless sensing encodes physiological and behavioral information about the people in the sensing environment: heart rate and breathing pattern, sleep monitoring, gesture, presence and movement, and even speech reconstructed from object vibrations [6], [7], [8]. Depending on where these systems are deployed, the same data can have very different privacy implications. For example, through the lens of contextual integrity [9], a Google Nest Hub monitoring the owner's sleep might meet the standard norms, while the same device at an Airbnb inadvertently monitoring the guest's sleep does not.

As more and more wireless sensing systems are being deployed and becoming more powerful, conversations about the privacy aspect of this technology are not advancing at the same pace. We need secure and trustworthy systems. In this reflection I want to sketch two design choices toward that goal: user opt-in vs system enforced. Both reflect a long-standing distinction in privacy theory: privacy as something the individual is asked to defend [10], [11], versus privacy as something built into the system [12], [13].

The first camp, user opt-in, is necessary when the subject does not own or control the sensor in the room, for example a guest in someone else's home or a visitor in a public space. The user needs to have a device that adds decoy or obfuscating signals into the sensor's view, so that an unauthorized sensor only recovers a plausible but wrong reading while authorized sensors keep working as usual. The advantage is that the user controls their own protection and does not have to trust the operator of the sensor. The drawback is that the user must wear or carry something, the protection is only as good as the obfuscation, and it does not extend to other people in the same room.

System-enforced protections are built into the sensing platform itself, so that even the operator cannot learn beyond what is authorized. In practice, wireless sensing is usually split across two layers: a lightweight edge device like a small radar module or a Wi-Fi router that captures the raw signal, and a cloud backend that does the heavy signal processing and inference. This edge-cloud architecture is well suited for sensing systems because vital-sign monitoring, gesture recognition, and activity classification increasingly involve complex models that the edge device cannot run on its own. The challenge is that as soon as the raw signal leaves the device for the cloud, the cloud sees everything the signal carries, and the flow of information is not so straightforward anymore.

Cryptographic and hardware-based approaches can address this problem by protecting the information flow in the cloud with cryptographic hardness or hardware security. Fully homomorphic encryption (FHE) [14] lets the cloud run the sensing pipeline directly on

encrypted data, so the heavy compute still happens off the device but the cloud never sees the underlying signal. Trusted execution environments (TEE) [15] take a weaker but cheaper approach, where the sensitive computation runs inside a secure enclave that even the cloud provider cannot inspect, in exchange for trusting the chip vendor. A related tool is differential privacy (DP) [16], which is particularly relevant for the emerging sensing foundation models, bounding how much information about any individual subject can leak from the model the system eventually deploys. The advantage of system-enforced cloud protections is that the user does not have to do anything, and the protection extends across all users of the deployment at once [12]. These protections in the cloud come at the higher cost of computational complexity of processing and inference compared to typical implementations.

The next generation of wireless networks is being designed around Integrated Sensing and Communication, or ISAC, in which 6G base stations and Wi-Fi access points are envisioned to act as passive sensing radars [17]. Going forward, neither user opt-in nor system enforcement is enough on its own. Opt-in protects the subject who was never asked. System enforcement protects the subject who was asked for something specific, but is now being sensed for something completely different. Our group's recent work has explored both sides, PrivyWave [18] on the user-opt-in side and mmFHE [19] on the system-enforced side, with the goal of closing the privacy gaps that either side leaves on its own. Cutting-edge research in both directions, grounded by the relevant contextual norms in these deployments, is needed to inch towards the goal of truly secure and trustworthy human-centered wireless sensing systems.

References

- [1] "Learn about Sleep Sensing on Google Nest Hub (2nd gen) - Android - Google Nest Help." Accessed: May 21, 2026. [Online]. Available: <https://support.google.com/googlenest/answer/10357288?hl=en&co=GENIE.Platform%3DAndroid>

- [2] “SleepScore App | Track & Improve Your Sleep,” Sleep.ai. Accessed: May 21, 2026. [Online]. Available: <https://www.sleep.ai/sleepscore/>
- [3] “Pontosense | The Future of AI Sensing,” Pontosense. Accessed: May 21, 2026. [Online]. Available: <https://www.pontosense.com>
- [4] “Logitech Spot - Presence and Environmental Sensor.” Accessed: May 21, 2026. [Online]. Available: <https://www.logitech.com/en-us/products/video-conferencing/accessories/spot-sensor.html>
- [5] J. Yang *et al.*, “MM-Fi: Multi-Modal Non-Intrusive 4D Human Dataset for Versatile Wireless Sensing,” *Adv. Neural Inf. Process. Syst.*, vol. 36, pp. 18756–18768, Dec. 2023.
- [6] J. Zhang *et al.*, “A Survey of mmWave-Based Human Sensing: Technology, Platforms and Applications,” *IEEE Commun. Surv. Tutor.*, vol. 25, no. 4, pp. 2052–2087, 2023, doi: 10.1109/COMST.2023.3298300.
- [7] Y. Ma, G. Zhou, and S. Wang, “WiFi Sensing with Channel State Information: A Survey,” *ACM Comput. Surv. CSUR*, vol. 52, no. 3, p. 46:1-46:36, Jun. 2019, doi: 10.1145/3310194.
- [8] P. Hu, W. Li, R. Spolaor, and X. Cheng, “mmEcho: A mmWave-based Acoustic Eavesdropping Method,” in *Proceedings of the ACM Turing Award Celebration Conference - China 2023*, in ACM TURC ’23. New York, NY, USA: Association for Computing Machinery, Sep. 2023, pp. 138–140. doi: 10.1145/3603165.3607440.
- [9] H. Nissenbaum, “7. Contexts, Informational Norms, Actors, Attributes, and Transmission Principles,” in *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2020, pp. 129–157. Accessed: May 21, 2026. [Online]. Available: <https://www.degruyterbrill.com/document/doi/10.1515/9780804772891-012/html?lang=en>
- [10] D. J. Solove, “Introduction: Privacy Self-Management and the Consent Dilemma,” Harvard Law Review. Accessed: May 21, 2026. [Online]. Available: <https://harvardlawreview.org/print/vol-126/introduction-privacy-self-management-and-the-consent-dilemma/>
- [11] P. M. Regan, “Privacy as a Common Good in the Digital World,” *Inf. Commun. Soc.*, vol. 5, no. 3, pp. 382–405, Jan. 2002, doi: 10.1080/13691180210159328.

- [12] K. Yeung, “Can We Employ Design-Based Regulation While Avoiding Brave New World?,” *Law Innov. Technol.*, vol. 3, no. 1, pp. 1–29, Jul. 2011, doi: 10.5235/175799611796399812.
- [13] M. Hildebrandt, “Algorithmic regulation and the rule of law,” *Philos. Trans. R. Soc. Math. Phys. Eng. Sci.*, vol. 376, no. 2128, p. 20170355, Aug. 2018, doi: 10.1098/rsta.2017.0355.
- [14] P. Martins, L. Sousa, and A. Mariano, “A Survey on Fully Homomorphic Encryption: An Engineering Perspective,” *ACM Comput. Surv. CSUR*, vol. 50, no. 6, p. 83:1-83:33, Dec. 2017, doi: 10.1145/3124441.
- [15] P. Jauernig, A.-R. Sadeghi, and E. Stäpf, “Trusted Execution Environments: Properties, Applications, and Challenges,” *IEEE Secur. Priv.*, vol. 18, no. 2, pp. 56–60, Mar. 2020, doi: 10.1109/MSEC.2019.2947124.
- [16] C. Dwork, “Differential Privacy,” in *Encyclopedia of Cryptography, Security and Privacy*, Springer, Cham, 2025, pp. 649–652. doi: 10.1007/978-3-030-71522-9_752.
- [17] “ISAC.” Accessed: May 21, 2026. [Online]. Available: <https://www.qualcomm.com/research/6g/isac>
- [18] Y. Gao, T. Ahmed, Z. Chang, T. Roumen, and R. Nandakumar, “PrivyWave: Privacy-Aware Wireless Sensing of Heartbeat,” Nov. 06, 2025, *arXiv*: arXiv:2511.02993. doi: 10.48550/arXiv.2511.02993.
- [19] T. Ahmed, Y. Gao, A. Armouti, and R. Nandakumar, “mmFHE: mmWave Sensing with End-to-End Fully Homomorphic Encryption,” *arXiv.org*. Accessed: May 21, 2026. [Online]. Available: <https://arxiv.org/abs/2603.22437v1>

Tanvir Ahmed
DLI Doctoral Fellow
ta376@cornell.edu
[More Info >](#)