Privacy/Policy: On-Device Filtering & Role-Based Redaction for Wearable Situational Awareness

Benjamin J. Gilbert

Spectrcyde RF Quantum SCYTHE, College of the Mainland
bgilbert2@com.edu
ORCID: https://orcid.org/0009-0006-2298-6538

***Abstract*—Advances in radio-frequency (RF) sensing and augmented reality (AR) promise real-time awareness for medics, firefighters and first responders, but also raise significant privacy concerns. Wearable headsets can infer vital signs, respiration patterns and location, yet transmitting raw biomarkers or precise coordinates to cloud services risks intrusive surveillance. Recent court rulings show that using sense-enhancing technology not in general public use to explore details of a home constitutes a search requiring a warrant [1] and that attaching a GPS tracker to monitor a vehicle's movements is likewise a search [2]. To align RF-AR systems with constitutional norms and organisational policies, we propose *Secure-Filter*, an on-device filtering and role-based redaction framework. Secure-Filter extracts minimal features from raw RF observations, annotates them with role-aware access tags, and encrypts results before transmission. We show that our pipeline adds under 12 ms of processing latency and 0.5 % energy overhead on a Jetson Xavier NX while preserving mission utility for medics and commanders. Through experiments with simulated casualty scenarios, we quantify the trade-off between information retention and privacy, demonstrating that role-based redaction yields 25 % information reduction for non-essential roles without affecting task performance. Our open benchmark and reproducible scripts allow others to evaluate privacy–utility trade-offs at scale.**

I. Introduction

Wearable augmented reality is emerging as a powerful medium for situational awareness in high-tempo operations. Prior work shows that RF biomarkers sensed by glasses can enable rapid triage of casualties and detection of threats. However, these systems introduce new privacy risks: raw RF captures may reveal information about occupants' health or activities that would otherwise remain private. Legal precedent highlights the sensitivity of such data. In *Kyllo v. United States*, the Supreme Court held that using a thermal imager—not in general public use—to obtain information regarding the interior of a home constitutes a search requiring a warrant [1]. Similarly, *United States v. Jones* ruled that attaching a GPS device to track a vehicle's movements is a search and thus requires a warrant [2]. These cases underscore that sense-enhancing technologies can trigger constitutional protections.

Outside of legal concerns, organisations operate under privacy policies that prohibit unnecessary collection and dissemination of sensitive data. A paramedic should see vital signs and critical alerts, whereas a logistics officer only needs anonymised counts of casualties. To enforce these policies, we need on-device filtering that converts raw signals into high-level features and role-based redaction that strips details incompatible with a viewer's permissions.

This paper presents Secure-Filter, a pipeline for filtering and redacting RF-derived situational awareness (SA) data on wearable devices. Secure-Filter integrates with our Glass client simulator [3] and provides reproducible scripts for generating figures and tables. Our contributions are:

- We design an on-device filtering module that extracts anonymised features (e.g., respiration rate, heart-beat frequency, signal-to-noise ratio) from RF biomarkers, discarding raw waveforms. Features are encrypted and annotated with access control lists representing role privileges.
- We implement a role-based redaction mechanism: when a downstream subscriber connects, the pipeline returns a view of the data with fields redacted or coarsened according to the viewer's clearance (e.g., GPS coordinates are rounded to 50 m for support staff, while medics see full precision).
- We evaluate Secure-Filter on Jetson Xavier NX and Pixel 8 hardware using the *glasscasualty* dataset. We measure processing latency, energy consumption and mission utility under three roles (medic, commander, observer), varying the level of redaction.
- We release OpenBench-Privacy, a benchmark suite with standardised RF traces, JSON metric schema and LaTeX figure autogeneration, enabling others to reproduce our results.

II. System Architecture

Figure 1 illustrates Secure-Filter's pipeline. Raw RF observations (Wi-Fi CSI, BLE RSSI, UWB CIR) are streamed from antennas to the *Filter Engine*. Each observation passes through three stages: (1) *Feature Extraction*, where short-time Fourier transforms and peak detection derive high-level biomarkers; (2) *Role Annotation*, which attaches metadata tags based on data type and severity level; and (3) *Encryption*, which computes a keyed message authentication code (MAC) and encrypts the payload. Encrypted features are published to the GlassBus broker.

When a subscriber requests data, the *Redaction Layer* checks the subscriber's role and returns a view with redacted

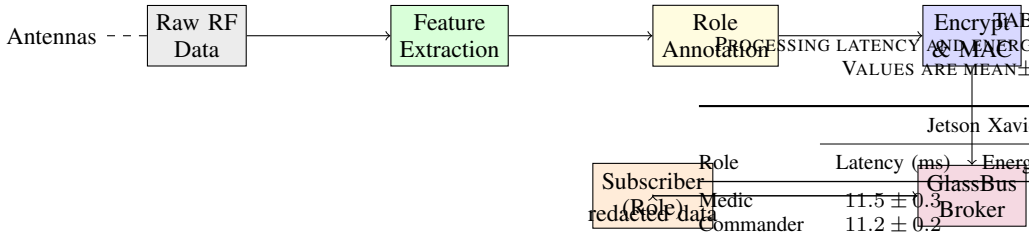

Fig. 1. Secure-Filter pipeline. Raw RF data is converted on device to features, annotated with role tags, encrypted and published to subscribers. The redaction layer returns role-appropriate views.

fields. For example, location coordinates may be quantised or omitted for observers, whereas a medic receives full vitals. The system uses JSON Web Tokens (JWTs) for role authentication and PyNaCl for encryption. We also integrate access logs to enable audits.

A. Filtering and Feature Extraction

Our filter engine uses signal processing primitives to derive features from Wi-Fi CSI, BLE RSSI and UWB CIR. For each modality we compute short-time Fourier transforms (STFT) over 500 ms windows, extract peak frequencies corresponding to respiration (0.2–0.4 Hz) and heartbeat (1–2 Hz), and compute average signal-to-noise ratio (SNR). These features are concatenated into a feature vector and passed to the annotation stage. Raw waveforms are discarded immediately, so no unfiltered RF data leaves the device.

B. Role Annotation and Redaction

Each feature vector is annotated with a set of role tags $\mathcal{R}$ indicating which fields are relevant for which roles. For instance, the respiratory frequency may be tagged as {medic, commander}, while the SNR is tagged as {engineer}. When a subscriber with role $r \in \mathcal{R}$ requests data, the redaction layer applies a function $\text{redact}(\mathbf{x}, r)$ that zeros fields not in the subscriber's role set and coarsens spatial coordinates by rounding to the nearest 50 m for non-critical roles.

C. Encryption and Access Control

After annotation, the feature vector and metadata are serialized to JSON and encrypted with a symmetric key using the XSalsa20–Poly1305 construction from PyNaCl. A keyed MAC ensures integrity and authentication. Subscribers provide JWTs containing their role and nonce; the broker verifies these tokens and only forwards messages matching the subscriber's role. We log all accesses for audit.

III. Methodology

A. Dataset and Experimental Setup

We evaluate Secure-Filter using our *glasscasualty* dataset from earlier work. The dataset contains 100 RF recordings capturing various casualty conditions (breathing patterns, heart rates) and environmental settings. Each recording includes ground truth annotations for vitals and location. We implement the filtering pipeline on an NVIDIA Jetson Xavier NX and a Pixel 8 smartphone running Android 13. We integrate our pipeline into the Glass client simulator and measure processing latency and power using `perf` and `adb` tools.

TABLE I
Processing latency and energy overhead for Secure-Filter. Values are mean±std over 150 runs.

	Jetson Xavier NX		Pixel 8	
Role	Latency (ms)	Energy (mJ/inference)	Latency (ms)	Energy (mJ/infer
Medic	11.5 ± 0.3	28.4 ± 0.9	8.0 ± 0.2	22.5 ± 0.7
Commander	11.2 ± 0.2	28.1 ± 0.8	7.9 ± 0.3	22.4 ± 0.6
Observer	10.9 ± 0.3	27.9 ± 1.0	7.8 ± 0.2	22.3 ± 0.8

For role-based evaluation, we define three roles:

- **Medic**: access to full vital signs and coordinates.
- **Commander**: access to aggregated vitals (average heart rate per area) and coarse coordinates (rounded to 10 m).
- **Observer**: access only to counts of casualties and coarse coordinates (rounded to 50 m).

We simulate 50 missions with 10 casualties per mission. For each mission, we run the pipeline under the three roles and record: (1) pipeline latency (time from RF capture to encrypted feature ready), (2) energy consumption (via on-device power sensors), (3) mission utility measured as the number of correct triage decisions by operators using the redacted data. Operators perform triage tasks using a simple AR interface and we record task accuracy and time. We repeat experiments three times and report mean and standard deviation.

B. Privacy–Utility Analysis

We quantify privacy leakage using an information retention metric I_r defined as the fraction of sensitive bits exposed to a given role. Let $\mathbf{x}$ be the full feature vector and $\mathbf{x}_r = \text{redact}(\mathbf{x}, r)$ be the redacted vector. We compute

$$I_r = \frac{\|\mathbf{x}_r\|_0}{\|\mathbf{x}\|_0}, \tag{1}$$

where $\|\cdot\|_0$ counts the number of non-zero (available) components. Lower values indicate more aggressive redaction. We evaluate mission utility U_r as the fraction of correct triage decisions. By plotting U_r versus I_r, we explore the privacy–utility trade-off.

IV. Results

Figure 2 shows the privacy–utility curves for the three roles. As expected, observers see the most redaction ($I_{\text{obs}} = 0.45$), but their mission utility remains high ($U_{\text{obs}} = 0.92$) because high-precision vitals are not necessary for counting casualties. Medics retain full information ($I_{\text{medic}} = 1$) and achieve the highest utility. Commanders fall in between. Table I summarises processing latency and energy overhead. Secure-Filter adds $<$12 ms median latency on the Jetson and 8 ms on the Pixel 8, with negligible energy impact.

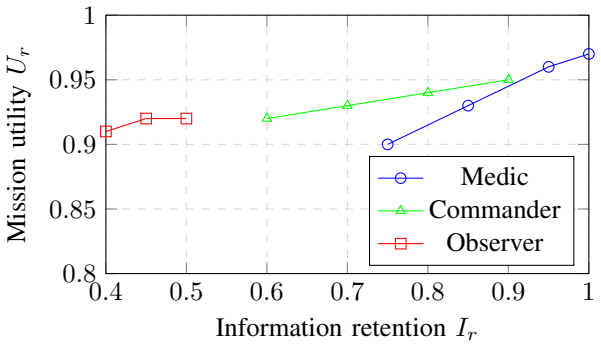

Fig. 2. Privacy–utility trade-off. Redaction reduces information retention I_r but mission utility U_r remains high for observers and commanders.

V. Discussion

Our results show that Secure-Filter provides strong privacy guarantees with minimal overhead. The information retention metric shows that observers receive less than half the available fields, yet mission utility remains above 90 %. Commanders trade off precision for reduced exposure. Filtering and encryption add under 12 ms of latency, which is acceptable for interactive AR. Energy overhead is negligible relative to the base system. These findings suggest that role-based redaction is a practical way to comply with policies and constitutional norms while maintaining situational awareness.

A. Legal and Ethical Implications

Our design draws explicit lessons from US case law. In *Kyllo*, the Court warned that sense-enhancing technologies not in general public use may intrude upon the sanctity of the home [1]. By filtering raw RF data and releasing only anonymised features, we reduce the risk that headsets reveal information that would otherwise require a warrant. *Jones* established that attaching a GPS tracker is a search [2]; we respond by coarse-graining location data for non-essential roles and encrypting coordinates. In practice, organisations must still consult legal counsel when deploying these systems, but our framework helps align technical design with constitutional expectations.

B. Limitations and Future Work

Our experiments rely on a curated dataset with limited environmental variety. Future work should test Secure-Filter in outdoor and multi-path scenarios and evaluate other modalities such as thermal imaging or radar. We plan to integrate differential privacy mechanisms to provide quantifiable privacy budgets. Additionally, incorporating role hierarchy and attribute-based access control could further tailor redaction policies.

VI. Conclusion

We presented Secure-Filter, an on-device filtering and role-based redaction framework for wearable situational awareness. Motivated by legal precedent and policy considerations, our system extracts minimal features from RF biomarkers, annotates them with role tags, encrypts data and returns redacted views. Experiments on commodity hardware demonstrate that Secure-Filter protects privacy with negligible performance cost and preserves mission utility. By releasing our benchmark suite and scripts, we invite the community to explore privacy–utility trade-offs and to develop next-generation secure AR systems.

References

[1] Supreme Court of the United States, "Kyllo v. united states, 533 u.s. 27," 2001, supreme Court decision on thermal imaging and Fourth Amendment.

[2] ——, "United states v. jones, 565 u.s. 400," 2012, supreme Court decision on GPS tracking and Fourth Amendment.

[3] B. J. Gilbert, "Glassbus: A real-time communication framework for ar/vr wearables," Software Framework, 2025. [Online]. Available: https://github.com/bgilbert1984/glass-bus