ISAC Privacy: Challenges and Solutions for 6G

Onur Günlü[1,2], Stefano Tomasin[3], João P. Vilela[4], Francesco Chiti[5], Prajnamaya Dass[6], Angeliki Alexiou[7], and Utz Roedig[8]

[1] Lehrstuhl für Nachrichtentechnik, TU Dortmund, Germany
[2] Information Theory and Security Laboratory (ITSL), Linköping University, Sweden
[3] Dept. of Information Eng. and Dept. of Mathematics, University of Padova, Italy
[4] INESCTEC, CISUC, and Dep. of Computer Science, Faculty of Sciences, University of Porto, Portugal
[5] Department of Information Engineering, University of Florence, Italy
[6] Barkhausen Institut, Dresden, Germany
[7] Department of Digital Systems, University of Piraeus, Greece
[8] School of Computer Science and Information Technology, University College Cork, Ireland

onur.guenlue@tu-dortmund.de, stefano.tomasin@unipd.it, jvilela@fc.up.pt, francesco.chiti@unifi.it, prajnamaya.dass@barkhauseninstitut.org, alexiou@unipi.gr, u.roedig@ucc.ie

Abstract. Integrated sensing and communication (ISAC) is a promising feature of future communication networks. While spatial sensing can improve network performance and enable external services, it also creates privacy challenges that go beyond the confidentiality of communication content. Future networks using millimeter-wave (mmWave) and sub-terahertz (THz) frequencies may collect or infer detailed information about people, devices, bystanders, passive objects, and environments in a sixth-generation (6G) deployment area. Such sensing can reveal location and environment data, support behavioral profiling such as movement or activity recognition, and, in advanced cases, expose physiological information such as breathing frequency or heart-rate-related data. Thus, the capabilities of spatial sensing must be controlled to satisfy privacy requirements. In this work, we organize privacy-sensitive ISAC data into three sensing levels: location and environment data, behavioral data, and physiological data, and use this classification as the organizing principle throughout the paper. Based on this classification, we discuss internal and external ISAC applications, identify privacy challenges related to consent, transparency, data ownership, profiling, bystander exposure, and sensitive sensing data, review representative solution directions, and outline future research directions for privacy-preserving ISAC.

Keywords: Integrated Sensing and Communication · 6G Networks · Privacy Preservation · Privacy-aware Sensing Data · User Profiling.

1 Introduction

Integration of sensing and communication operations will be a key component of future communication networks [11, 19]. Usually, spatial sensing is assumed

when referring to the term integrated sensing and communication (ISAC), also called joint communication and sensing (JCAS). Spatial sensing can be used within the network to improve performance, but it may also be used to provide external services. For instance, spatial sensing within the network can enable identification of temporary obstructions within a communication link, and the network could then take actions to react to the situation and change transmission arrangements. Similarly, external applications can make use of spatial sensing, such as traffic management systems that map the positions of vehicles and pedestrians [1, 35].

Spatial sensing via a network infrastructure is of particular interest due to the possibility of reusing parts of an already deployed communication infrastructure. Moreover, future networks are expected to use millimeter-wave (mmWave) and sub-terahertz (THz) frequencies, large antenna arrays, and directional transmission, which can support more accurate sensing and localization [18, 19, 67]. Using such high frequencies requires beamforming to enable communication over a larger distance, enabling networks to scan an area using a narrow beam. Thus, a future communication network may provide many of the elements required to build a radar-like system with dense infrastructure and wide-area coverage. These same capabilities, however, also make it necessary to control when, how, and for which purpose sensing is performed.

While implementing ISAC systems enables network optimization and new applications, it also introduces new security and privacy challenges [22,34,40,46,57]. Security challenges include deliberate manipulation of the sensing components of the network and attacks that degrade communication or sensing reliability. Besides security issues, the introduction of ISAC creates significant privacy challenges. Indeed, ISAC involves the collection and processing of sensing and situational data, including personally identifiable information; it poses major privacy risks [1, 8, 46]. In this work, we focus on the privacy implications of sensing-derived personal and environmental information, and discuss ISAC privacy challenges, representative solution directions, and future research trends. Here, we define a privacy breach as the loss of control over information about a person, their device, or their surrounding environment that is revealed through sensing. Thus, disclosure of the *content* of a communication message is not considered a privacy issue in this paper, but rather a confidentiality and security issue. Moreover, a person affected by ISAC sensing need not be an active network user, as passive objects and bystanders in the sensing area may also be included in sensing results [1, 8]. The discussion in this work covers sensing performed by base stations, cooperative network nodes, user equipments (UEs), or combinations thereof.

Communication networks already gather large amounts of user information, such as user identifiers, traffic patterns, access times, and locations. However, when this information is combined with fine-grained spatial sensing information, a new level of privacy loss can occur. In this work, we organize these risks and the subsequent discussion according to three privacy-sensitive sensing-data levels: (i) location and environment data, (ii) behavioral data, and (iii) physiological

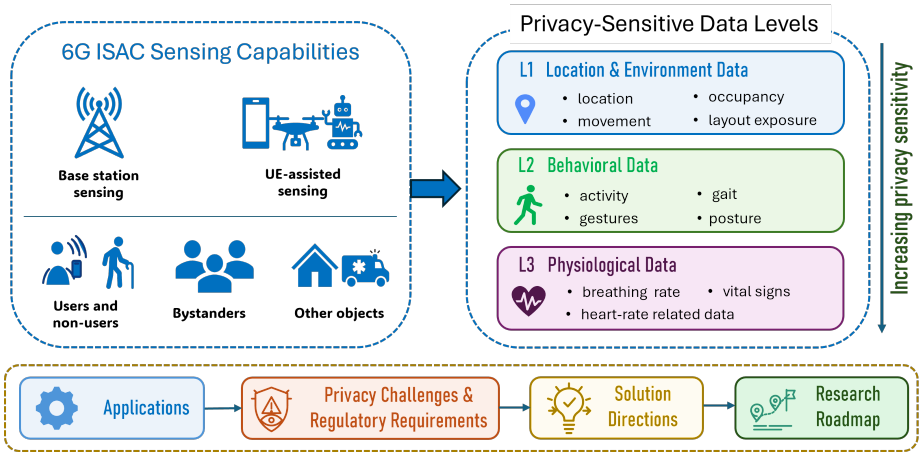


Fig. 1. Conceptual overview of this work's perspective on 6G ISAC privacy across base station-based and UE-assisted sensing. The figure highlights that this paper focuses on sensing-derived personal data rather than message content, organizes privacy-sensitive ISAC data into three levels (L1: location and environment data, L2: behavioral data, and L3: physiological data), and relates these levels to applications, privacy challenges, solution directions, and the research roadmap.

data. Given the resolution expected from mmWave and sub-THz sensing, it can be possible to infer location and movement [15, 44], behavior patterns such as gait, posture, gestures, or physical activity [30, 37, 42, 56, 62], and physiological parameters such as breathing frequency or heart-rate-related information [45, 48, 68]. Recent advances in artificial intelligence (AI) can further support the analysis of large sensing datasets and the creation of detailed profiles of people and environments [53, 60]. Furthermore, it will be difficult for people to avoid being sensed (e.g., by not carrying a phone), because mere presence in an area with sixth-generation (6G) coverage can subject them to sensing activity.

As future 6G networks will be ubiquitous, it is necessary to design them with respect to user privacy. This is essential to ensure that users will trust and accept the deployment of networks that have the potential to infringe on their rights to privacy. To this end, the capabilities of spatial sensing may have to be balanced with privacy requirements such as sensitive data minimization, consent, transparency, purpose limitation, access control, and secure handling of personal data [4, 6, 8, 17].

Recent tutorial and survey papers have covered ISAC signal processing, applications, network architectures, secure ISAC, and security/privacy challenges [19, 33, 40, 57, 58, 63–65, 70]. This work is complementary to those works, as it treats privacy as control over sensing-derived personal data and uses the three sensing-data levels introduced in Section 2.3 as the organizing principle. Fig. 1 provides a visual overview of this organizing principle.

In this work, we provide a brief overview of the envisioned ISAC technology for 6G networks. Next, we outline applications for ISAC, as it is essential

to consider specific applications when considering privacy challenges. We then provide a structured discussion of privacy challenges, including consent, transparency, data ownership, location and environment data, behavioral data, and physiological data. This is followed by an overview of currently available solution directions. We also describe privacy-related research areas that must be addressed in the future to ensure that users will trust and accept ISAC.

2 Sensing in 6G Networks

This section identifies the sensing capabilities needed to define the privacy-sensitive sensing-data levels used throughout this work.

2.1 6G Networks

The evolution of usage scenarios from fifth-generation (5G) to 6G, as recommended by the International Telecommunication Union (ITU) in [24], includes a group of extreme evolutions of the well-known 5G usage scenarios (mobile broadband (MBB), ultra reliable low latency communications (URLLC), massive machine type communications (mMTC)) towards immersive and hyper reliable connectivity and a group of three revolutionary usage scenarios with a clear emphasis on 'beyond communications' objectives, such as ubiquitous coverage, artificial intelligence, and cyber-physical interaction with the internet of senses (IoS).

The newly introduced usage scenarios, in particular ubiquitous connectivity, ISAC, and integrated AI and communication, introduce a major paradigm shift [19, 24]. Connectivity in next-generation networks will not be only about transmission of bits: monitoring the environment, detecting and tracking mobility, localization, shape identification, and semantic understanding are among the targeted functionalities. Moreover, the adoption of AI/Machine Learning (ML) can support the analysis of complex and stochastic radio environments. Note that with ISAC we refer to the reconstruction of the surrounding electromagnetic environment, in particular of the passive targets that are not active devices but objects (and people) hit by electromagnetic signals emitted by network devices (base stations or UEs). In this context, situational awareness, environmental sensing, tunability, and learning become central capabilities. More importantly, to assess such beyond-communication capabilities, 6G technical performance requirements need to go beyond traditional metrics such as data rate, spectral efficiency, latency, and reliability, and include sensing- and AI-related metrics, positioning accuracy, energy efficiency, and resilience [11, 24].

Defining quantitative measures for the new 6G capabilities is a challenging task, mainly because target values are hard to determine and are highly dependent on the specific use case and application. Even more important is the definition of the overarching objectives and strategic priorities in the design and deployment of 6G networks. As emphasized by the ITU, sustainability, "connecting the unconnected", and security and privacy are defining key values that 6G is expected to serve.

2.2 Sensing Approaches

In the 6G era, the conventional view of the network as a manager of physical and virtual resources is expected to evolve toward a system that supports programmability, power efficiency, resilience, intelligence, and sensing-as-a-service within an integrated communication-and-sensing architecture. Realizing such co-designed communication and sensing requires: (i) propagation and channel modeling principles, waveforms, signaling, protocols, and algorithms for ISAC; (ii) sensing beyond conventional sensor/actuator and radar concepts, where communication systems also support beyond-communication functionalities; and (iii) integration of sensing technologies, ISAC, and AI/ML capabilities into a wireless network optimization framework [32, 33, 64, 65].

Radio frequency sensing and wireless communications have traditionally been performed in separate systems, in distinct platforms and in non-cooperative settings [33, 64]. They have different objectives and performance criteria, for example, data rate or quality of service in communications, and detection probability or the Cramer-Rao bound of target parameter estimation for sensing. Radio frequency sensing can be passive, as in localization via passive radars that may use communication signals as signals of opportunity, or active, where sensors probe their operational environment by emitting self-generated energy and observe the signals reflected off the targets as in active radars or radio frequency imaging. The sensing tasks involve target detection, tracking, target recognition, imaging, and channel and direction of arrival estimation, which are then directly used to aid communication tasks, such as data symbol estimation, or beamforming to enhance signal-to-noise ratio and mitigate interference. For the purpose of this paper, these sensing tasks are important because their outputs can become location, environment, behavioral, or physiological information rather than only communication-side state information.

In 6G, sensing will be used to obtain situational awareness in order to enhance communications performance [11, 19, 32]. For example, by utilizing radio environment sensing, transceiver operational parameters can be optimized or estimated, and consequently, communication performance can be improved. For instance, knowledge of the locations of mobile users can simplify beam alignment and allow for managing interferences in the spatial domain. A key component of designing sensing-aided communications is to build and maintain awareness in a dynamic radio environment. Optimizing waveforms to be suitable for both sensing and communication tasks and incorporating adaptability and prediction through AI/ML have an important role to play. In addition to the incorporation of sensing and radar capabilities into communication systems and the exploitation of sensing information to enhance communication performance, 6G is anticipated to offer a revolutionary path towards perceptive intelligence by introducing the notion of network-(nodes)-as-a-sensor. The use of a single base station for sensing the environment and the cooperation of multiple network nodes (access points or remote radio heads) opens new ways to improve the sensing performance [19, 65]. Moreover, the mobile users may serve either as sensors or sources of radio signals to be exploited by the network to perform sensing.

For example, cell-free network architectures, by exploiting signaling from multiple base stations and mobile stations, may enhance the sensing ability and provide sensing services, such as positioning of active users and mapping of the propagation environment, including blockage profiling. From a privacy perspective, this is important because sensing is no longer confined to dedicated radar devices or base stations, as cooperative network nodes and, in some settings, UEs may also contribute to the sensing process.

Motivated by the consideration of high frequency bands (mmWave and sub-THz), the adoption of large antenna arrays (LAAs) and large aperture reconfigurable intelligent surfaces (RIS) promise attractive solutions for extreme spatial reuse, pencil beamforming, and transceiver tunability [18, 50, 67]. Moreover, as the aperture of LAAs increases, the Fraunhofer distance increases as well and they operate in the near field (spherical waves) for several scenarios of interest (at substantial distance from the transmitter). Near field communications with LAAs offer the possibility to perform advanced wavefront engineering, involving phase shifts beyond the simple linear phase gradient that is required for conventional beam steering. For example, bending beams [14] are able to propagate along a curved trajectory, while beams with self-healing properties are able to reconstruct after being interrupted by a small blocker. Focused beams, on the other hand, are ideal for controlling power density in small focal areas, which is a key feature for localization [51], mobility tracking and sensing applications [50].

2.3 Privacy Sensitive Sensing Data

From the aforementioned overview on sensing technology for 6G, it is clear that privacy-sensitive information can be captured on different levels of granularity. We differentiate three levels of sensing granularity and, thus, resulting sensing data, linked to the capability of the present 6G deployment. The levels describe the type of information revealed, irrespective of whether the sensing data are generated by infrastructure nodes, UEs or both.

L1) *Location and Environment Data:* Tracking objects and people is the simplest (least technologically challenging) form of ISAC. Such a system can provide information on user location and movement [7, 63], revealing other private information, such as the visited places and meetings among different users. It can also sense the surroundings, which may disclose other privacy-sensitive information, such as the floor plan of a residence.

L2) *Behavioral Data:* More technologically advanced sensing systems can also record behavioral information on users. For example, they can determine the user posture, distinguishing between sitting, standing, or lying down (sleeping) users [69]. The movement of limbs may also be identified [59], and gait can be characterized, not only for users' identification but also to reveal their actions. It is also possible to determine what a user is touching. Note that while information about who a user meets could also be considered behavioral, we assign it to L1 because it primarily follows from location and movement information.

L3) *Physiological Data:* The most privacy-related challenge in sensing is the acquisition of physiological data, including breathing frequency and heart rate [61, 68]. Despite the persisting complexity of these tasks, the advent of sophisticated hardware, such as multiple antennas, and software, including signal processing techniques and machine learning algorithms, has led to significant advancements. The imminent availability of higher radio frequencies, characterized by enhanced spatial resolution, further augments the potential of 6G networks to provide such information. Evidently, the disclosure of such information is indicative of health data and may be regarded as particularly critical from a privacy standpoint, as stipulated in the general data protection regulation (GDPR).

It might be possible to avoid some privacy issues by limiting the 6G network at deployment to a specific level of sensing capability. However, that may not always be possible or desirable, and other privacy-preserving solutions must be integrated within the network. We discuss some of these in Section 5.

In the next sections, we use the aforementioned classification to structure our discussions on sensing applications, privacy challenges, and solutions.

3 Sensing Applications

Sensing is widely expected to provide efficiency, reliability, and contextual intelligence to the network by integrating and coordinating sensing capabilities and communication technologies [32]. Sensing applications can be categorized according to their scope. *Internal* applications use sensing to optimize or protect the operation of the network itself, whereas *external* applications rely on sensing as an enabler for vertical services beyond network operation. In this work, we identify representative internal and external applications according to the privacy-sensitive sensing-data levels introduced in Section 2.3.

3.1 Internal Applications

Internal applications of ISAC envision improving network operation and performance, for example, through detection and adaptation of communication states and security threat classification/mitigation through network-based monitoring.

Communications State Detection and Adaptation. The utilisation of ISAC can provide insights into the received signal, channel conditions, interference sources, and environmental factors. The real-time access to such information can be exploited to dynamically adapt the communication transmission parameters (e.g., waveform design, modulation scheme, bandwidth, and power allocation) on a link basis, or even to apply a cluster of RISs in a coordinated manner to achieve end-to-end optimised connectivity [31]. This application mainly relies on L1 data, because channel and environmental information may reveal location, movement, blockage, and occupancy-related information.

Security Threat Classification and Mitigation. The accurate estimation of physical-layer features can support the detection and classification of attacks, with the aim of protecting communication and sensing functions against unauthorized entities [34, 41, 43].

In the context of ISAC, the network's sensing functionality can be used to monitor the radio environment for anomalous physical presences. For example, by analyzing high-resolution channel state information (CSI) and Doppler shifts, the system may identify entities that do not transmit but alter the propagation environment, and adapt the beamforming strategy accordingly to adaptively null the beam in the direction of the intruder [23].

This application primarily relies on L1 sensing, since environmental mapping and location-related information are used to detect anomalous objects or presences. Furthermore, recent advances in physical-layer security and ML-based monitoring can support the real-time classification and mitigation of sophisticated wireless threats, such as pilot contamination and smart jamming, in ISAC-related settings [34, 41, 43]. Thus, more advanced classification may also use features related to movement or device behavior, and therefore may involve L2 data.

3.2 External Applications

External applications use sensed network information to enable vertical-specific services beyond network operation. Representative scenarios include environmental monitoring, living-environment monitoring and control, and management of mobile agents. For each application class, we indicate the relevant sensing-data levels, L1-L3, defined in Section 2.3.

Environmental Monitoring (level L1). ISAC technology can be applied to environmental and climatic monitoring [1, 16, 60], including physical parameters such as temperature, humidity, and wind speed, as well as air or water quality, pollutant presence, and disaster monitoring, e.g., earthquakes, fires, and floods. In this work, this application is mainly associated with L1, because the sensed information concerns the physical environment rather than behavioral or physiological attributes.

Living Environments Monitoring and Control (levels L2 and L3). The improved precision of sensing capabilities in indoor scenarios can support intelligent living environments and human-to-machine interaction. In particular, by feeding the CSI data or derived features to ML models, CSI sensing can enable the recognition of large- and small-scale movements, such as activities, e.g., walking, running, and jumping, or gestures [30, 37, 42], as well as person identification [30, 39]. Applications include sign-language translation [37], human-machine interfaces in internet of things (IoT) applications, activity monitoring, and physiological-signal monitoring [60]. These applications mainly involve L2 data when activity, gesture, posture, or identity-related behavior is inferred, and L3 data when physiological signals are monitored.

Mobile Applications (levels L1 and L2). ISAC is a key enabler for mobile and highly dynamic scenarios in future 6G systems, where rapid environmental changes require coordination between perception and data exchange. In such settings, ISAC allows network nodes to infer spatial context while maintaining connectivity, supporting mobility-aware decision making for autonomous and connected agents [26, 32]. Specifically, for vehicular networks, ISAC enables the joint detection of the operating environment and neighboring mobile devices. This synergy supports advanced vehicle-to-everything (V2X) communication schemes, for example, in autonomous-agent platooning, where real-time sensing of surrounding gaps and velocities is important for stability and safety under dynamic traffic conditions [35]. Beyond road traffic, similar principles extend to coordinated operation of mobile agents such as unmanned aerial vehicles, where groups of mobile nodes can adapt their trajectories, avoid obstacles, and maintain formation without relying exclusively on external sensors [19]. The data gathered in these scenarios typically maps to L1 for environmental mapping and trajectory tracking, and may involve L2 when mobile objects, users, or hazards are characterized beyond their location and movement.

Industrial Site Coordination (levels L1 and L2). The distributed integration of communication and dynamic context-sensing capabilities among nodes can support collaboration in 6G intelligent factories [19]. This can improve the coordination of mobile agents, including workers, vehicles, robots, and cobots, and consequently enhance overall operational efficiency. In particular, mobility can be managed by using ISAC for trajectory tracking and hazard or obstacle detection in workplace-safety applications. Moreover, the inherent high data rates can support industrial virtual reality (VR)/augmented reality (AR) applications, where behavioral monitoring may enable immersive training, design, and maintenance tasks. Finally, ISAC can support closed-loop and real-time monitoring and control of industrial processes, including spatial and differentiated access control and predictive equipment maintenance. In these scenarios, L1 data arises from tracking, mapping, occupancy, and obstacle detection, whereas L2 data may arise when worker behavior, gestures, posture, or interaction patterns are inferred.

Emerging sensing-based applications, either internal or external, span sensing granularities from location and environment data L1 to behavioral data L2 and, in some cases, physiological data L3. These levels are useful for organizing privacy analysis because the same sensing information that enables network optimization, mobility support, living-environment control, or industrial coordination may also reveal information about users, devices, bystanders, passive objects, and environments. The following section, therefore, discusses the corresponding privacy challenges.

4 Privacy Challenges

This section identifies the privacy challenges that follow from sensing-derived personal and environmental information in ISAC. We first recall the relevant scope of personal data and profiling under the GDPR. We then discuss governance challenges in sensing-data handling, followed by risks associated with the three sensing-data levels introduced in Section 2.3. Note that in this section, the adversary can be of different types: from an honest-but-curious network operator to a rogue base station, from an unauthorized third-party application to a malicious bystander UE sniffing reflected waves.

4.1 Definitions and Scope

As specified in Section 1, this paper considers the disclosure or loss of control over sensing-derived personal or environmental information as a privacy breach, whereas the disclosure of message content is treated as a confidentiality and security issue. Not only active users, but also bystanders and passive objects in the target sensing area may be sensed, which can lead to the collection of sensitive contextual information [16]. To provide a more precise definition of the concept of privacy, we turn to the most recent literature on the subject, particularly the GDPR of the European Union. This regulatory instrument has established de facto global standards regarding privacy, defining *personal data* as [17, Art. 4] "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

ISAC can facilitate the acquisition of location data, movement-related information, and, in some applications, health-related information. Such data may support profiling, a concept further delineated in the GDPR. According again to [17, Recital 71], profiling "consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyze or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her." According to the GDPR, the practice of profiling is permissible only under specific conditions. Where profiling or solely automated decision-making has legal or similarly significant effects, GDPR imposes specific conditions and safeguards, which may include explicit consent or other legally recognized bases. In all cases, the use of personal data must be clearly delimited and supported by appropriate privacy-aware safeguards. For further insights into the legal aspects of ISAC see also [4]. Consequently, ISAC design should account for privacy requirements from the outset, including limits on sensing purpose, data access, processing, storage, and

disclosure. In this paper, we focus on the technical and architectural implications of these requirements rather than providing a legal analysis.

The European standardisation work on ISAC has examined the privacy issues and proposed new potential requirements to address these challenges in ISAC-enabled 6G systems [16]. On the other hand, several papers have also surveyed the privacy issues of ISAC in 6G networks [3,10,47,52,70], focusing on technical solutions to protect some aspects (such as location privacy or the leakage of the sensing signal to unauthorized receivers), rarely addressing the main and fundamental shortfalls of ISAC with respect to privacy. The Commonwealth Scientific and Industrial Research Organisation (CSIRO) has also issued a report [54] on security and privacy issues in 6G, including a discussion on ISAC. In contrast, this section organizes the privacy challenges according to governance requirements and the three sensing-data levels used throughout this work.

4.2 Governance Challenges in Sensing-Data Handling

Consent and Authorization for Sensing. In conventional communication systems, tracking is mainly associated with active and connected UEs. In contrast, ISAC extends the scope of observation to the surrounding physical environment, where sensing may lead to collateral data collection involving bystanders and passive objects. As a result, ISAC may enable the collection of personally identifiable information (PII) related not only to connected users, but also to individuals who do not carry or use a UE within the sensing environment [1,16].

Use cases involving 3GPP sensing in public areas, such as intruder detection on highways and railway crossings, tourist-spot traffic management, and UAV-based applications, may therefore involve the collection of PII related to human beings. In restricted or sensitive areas, such as military zones, sensing may further expose sensitive information, including geolocation data, operational activities, and infrastructure details. Therefore, where applicable and possible, consent or authorization from public management bodies and relevant authorities should be obtained before enabling 3GPP-based sensing services. In addition, when the network intends to use UEs as sensing entities or sensing-data providers, explicit user consent and appropriate privacy controls are required before such involvement [1,8,10].

Transparency, Purpose Limitation, and User Control. Depending on the application request, the network may collect sensing data from an area of interest and may also involve UEs in the sensing process. However, the purpose of sensing, the intended use of the sensing data, the processing entities involved, and the parties authorized to access the sensing results may not always be transparent to users or UE owners. In such cases, sensing may occur without sufficient authorization, purpose limitation, or user control.

For example, sensing data collected through UEs for pedestrian detection at crossroads may later be repurposed for commercial analytics, such as estimating traffic density near shopping malls. Similarly, users may be unaware

that movement-related information collected to improve traffic flow is also being used to support commercial decision-making or marketing strategies. Beyond the original sensing purpose, the disclosure of sensing results to third parties may also reveal PII related to users, UEs, and bystanders present in the sensing environment.

4.3 Location and Environmental Privacy Risks

The first sensing-data level L1 concerns location and environment data. A central privacy risk at this level is the ability of ISAC to localize and track moving or static objects. Different from localization techniques that are able to obtain the position of active transmitters (e.g., through triangulation and or trilateration), the sensing capabilities of ISAC enable the positioning of passive objects, and these include also people. In this case, communication signals may also be used for radar-like sensing. Such sensing can be difficult for affected individuals to detect, making transparency and control challenging.

ISAC systems have the capability to capture location data of users at varying levels of granularity, ranging from broader zones or areas to precise coordinates. There are different methods, such as time difference of arrival (TDoA), angle of arrival (AoA), angle of departure (AoD) measurements, received signal strength indicator (RSSI), etc., to detect and locate static and moving objects [1, 65]. The network operator can also combine location estimates over time to infer location histories. Base stations with sensing capabilities may also cooperatively track movement. In ISAC applications, such as pedestrian detection at crossroads and automotive maneuvering, the location of the users requesting the service is continuously monitored to identify any obstacles around them [1].

ISAC can also be used to determine occupancy of spaces and, when sensing features become more detailed, to infer activity or identity-related characteristics [49, 56]. These capabilities create a boundary between L1 risks, such as occupancy and presence detection, and L2 risks, such as activity or identity-related behavioral inference, including sensing through opaque obstacles [2].

4.4 Behavioral Profiling Risks

The second sensing-data level L2 concerns behavioral data. From sensing data captured in the environment, sensing units or network operators may infer behavior of users, UEs, or other objects in the sensing area [28].

While behavioral inference in ISAC applications can support user experience and health-related monitoring, it also poses significant privacy risks. For instance, it can enable surveillance of routine behaviors, including where users move, when they interact with others, and contextual information such as walking or sleeping habits, by observing phase and/or amplitude patterns of the CSI [15, 44]. Moreover, an adversary with access to ISAC sensing signals or reflected signals may analyze CSI patterns to infer behavioral properties of objects in the sensing area. Behavioral profiling may also concern the sensing process itself, including when sensing signals are transmitted, which area is sensed, and

which UEs are involved. If sensing requests are exposed, an adversary may further link applications to the types of sensing data they request.

4.5 Physiological and Biometric Privacy Risks

The third sensing-data level L3 concerns physiological and biometric information. ISAC systems may support the extraction of sensitive personal attributes from the sensed environment, including physical dimensions, biometric features, and physiological indicators. In applications such as domestic health and sleep monitoring, radar-based sensing can facilitate the estimation of vital signs, such as heart rate and respiration, and may also support biometric identification [45, 55]. Consequently, unauthorized sensing or misuse of ISAC infrastructure may expose personal attributes of humans or other targets within the sensing range. Such exposure of PII creates significant privacy risks, including identifiability and linkability threats [8, 13].

Note that under current frameworks (like the European Union AI Act), if a 6G base station processes radio data to classify human behavior (L2) or infer physiological vital signs (L3), the telecommunications operator is no longer a mere data conduit and it may become the operator of a high-risk biometric categorization AI system. This implies severe liabilities if “always-on" sensing occurs without a legal mandate.

5 Solutions to Privacy Challenges

Section 4 identified privacy risks that arise when sensing-derived information is collected, inferred, or disclosed. This section reviews representative solution directions and maps them to the three sensing-data levels introduced in Section 2.3. The emphasis is not on communication-message confidentiality, but on mechanisms that limit spatial observability at L1, restrict behavioral inference at L2, and control the collection, processing, and disclosure of highly-sensitive physiological or biometric information at L3.

5.1 L1: Location & Environment Privacy

At L1, privacy protection mainly concerns spatial observability: whether positions, movements, occupancy, or environmental structure can be inferred, and at what resolution. The representative mechanisms below therefore aim to reduce, obfuscate, or selectively control the spatial information available to unauthorized sensing receivers through signal processing and physical-layer techniques.

Location Obfuscation: Radio-based positioning techniques can achieve sub-meter localization accuracy [25], which creates privacy risks when users, bystanders, or passive objects can be localized without meaningful control. Location obfuscation addresses this risk by deliberately reducing the precision or reliability of the location information exposed by the sensing system.

For example, Nguyen et al. [44] propose mitigation strategies to control the precision, exposure, and usability of location information in sensing systems. They advocate privacy-aware positioning, where spatial and temporal resolution is deliberately limited based on application needs. Proposed solutions include location obfuscation, uncertainty-aware reporting, and access control mechanisms that restrict who can query location data and at what precision, supported by context-aware policies and user-centric privacy controls.

Keya et al. [27] propose a solution for ISAC systems based on channel obfuscation, where privacy is achieved by deliberately manipulating the wireless channel so that true user locations become indistinguishable from a predefined set of alternative locations. Specifically, the core idea is to control the resolution of location detection by transforming the Channel Frequency Response (CFR) such that the sensed signal associated with a true location becomes statistically close to signals corresponding to multiple "dummy" locations (an obfuscation set), increasing uncertainty for both passive and active attackers.

Artificial Noise Injection: Artificial-noise-based designs protect L1 privacy by degrading unauthorized sensing while preserving the intended sensing and communication functions. In this case, privacy is addressed by controlling the sensing information available to an unauthorized receiver.

Zou et al [71] consider the problem that the same dual-functional waveform used for legitimate sensing and communication can also be exploited by unauthorized receivers ("sensing Eves") to infer environmental and location information. The proposed solution is the introduction of a sensing-security framework based on beamforming and artificial noise (AN) injection, where sensing performance is intentionally controlled rather than universally maximized. The sensing mutual information of the legitimate sensing receiver is maximized while constraining the mutual information obtainable by an eavesdropper. To further suppress unauthorized sensing, the system injects artificial noise into the transmitted waveform, degrading the sensing quality and estimation capability of the Eve without significantly affecting the intended sensing and communication tasks.

RIS Based Approaches: RIS-assisted ISAC privacy approaches can actively manipulate the propagation environment to obfuscate sensing targets and reduce unauthorized localization accuracy.

The work by Magbool et al. [38] studies how RIS can be used to actively protect sensing privacy by reshaping the wireless environment. Instead of allowing all receivers to exploit high-resolution sensing signals, the RIS is configured to degrade the sensing quality at unauthorized observers, making targets harder to detect or localize, while still maintaining acceptable performance for legitimate users. This enables a form of selective sensing visibility, where spatial information, such as location and presence, becomes unreliable for adversaries. From a privacy perspective, the key benefit is that sensing accuracy itself becomes a controllable resource, allowing ISAC systems to deliberately introduce uncertainty into environmental and localization data without disabling sensing services altogether.

Directional Sensing Constraints: Directional constraints protect L1 privacy by making angular information less useful for localization while maintaining the communication link performance.

Khan et al. [29] propose a beamforming strategy that protects user location privacy by manipulating the angular characteristics of transmitted signals so that the true direction of arrival cannot be reliably inferred by a sensing receiver. Instead of simply reducing signal power, the method introduces a direction-of-arrival obfuscation power ratio (DoA-OPR) constraint, which ensures that misleading or false angular peaks dominate over the true direction in the received signal. By jointly optimizing communication performance and this obfuscation constraint, the approach allows the system to maintain reliable communication while distorting directional sensing information, effectively preventing accurate localization.

Ma et al [36] propose a physical-layer privacy mechanism that limits the ability of ISAC receivers to infer a transmitter's location by constraining the directional characteristics of the transmitted signal. Instead of maximizing beamforming gain toward a specific direction, the authors design a sensing-resistance beamformer that spreads or reshapes the angular power distribution to make the true direction less distinguishable.

5.2 L2: Behavioral Privacy (Activity, Gait, Gesture)

At L2, privacy protection concerns the inference of activity, gait, gesture, posture, identity-related behavior, or other behavioral patterns from sensing-derived data. The relevant solution directions therefore move beyond spatial obfuscation and focus on controlling the features, representations, model updates, or functions that are exposed to applications or other network entities. Emerging directions to address this are data-driven approaches that learn privacy-preserving representations, distributed and federated learning, and information-theoretic approaches that explicitly constrain the functions computed from sensing data.

ML-Based Privacy-Preserving Representation Learning: Privacy-preserving ML techniques, including adversarial learning, representation learning, and federated learning, are relevant for limiting sensitive inference in 6G systems [53]. In the present L2 context, such methods can be used to preserve task-relevant information, such as activity recognition, while reducing exposure of identity-related or behavioral attributes.

An example of this principle is given by Delgado-Santos et al. [12], proposing an approach based on autoencoders and adversarial training to transform gait data into privacy-preserving representations. The method preserves the utility of gait signals for authentication while suppressing sensitive attributes such as gender or contextual behavioral information, demonstrating how feature-level sanitization can mitigate behavioral privacy risks in sensing systems.

Distributed and Federated Learning: A complementary approach to protecting behavioral privacy in ISAC systems is to avoid centralized collection of behavioral sensing data. In distributed or federated learning architectures, raw sensing

data can remain at the device or network edge, while only model updates or aggregated parameters are shared. This can reduce the exposure of activity, gait, or gesture information to centralized entities.

For example, Zhang et al. [66] propose a federated-learning-based framework for WiFi CSI activity recognition that enables collaborative training across multiple environments without sharing raw sensing data. The proposed approach keeps local sensing data on-device or within the local environment, while only sharing learned model parameters for global training. Behavioral inference models can be collaboratively trained while limiting direct exposure of sensing data, reducing the risk of centralized behavioral profiling and unintended information leakage.

Privacy-preserving feature extraction and randomized inference: A further L2 direction is to restrict the behavioral functions computed from CSI, radar, or localization traces, instead of trying to protect raw measurements or unnecessarily detailed intermediate features. This is aligned with the privacy notion used in this paper, where the concern is loss of control over sensing-derived information that enables activity, gait, gesture, or posture inference.

Randomized function-computation models provide related conceptual tools for this direction. The randomized distributed function computation (RDFC) framework studies the synthesis of randomized functions of distributed data under privacy constraints [5, 20], while private remote-source function computation studies tradeoffs between function computation and information leakage for remote sources, such as semantics of data [21]. These works provide useful abstractions for future sensing pipelines in which applications receive only controlled, possibly randomized, sensing-derived outputs rather than full signal representations.

5.3 L3: Physiological Privacy (Vital Signs, Biometrics)

At L3, the privacy concern is the exposure of physiological or biometric information, such as breathing patterns, heart-rate-related features, or biometric identifiers. Compared with L1 and L2, protection at this level requires stricter data minimization and lifecycle control, because the information may be sensitive, persistent, and difficult to revoke once disclosed. The main design objective is therefore to limit collection where possible and, when collection is necessary, to tightly control processing, storage, access, and disclosure within ISAC systems.

The work by Dass et al. [9] proposes a privacy-preserving ISAC architecture in which sensing, processing, and data access are separated into controlled functional components. The architecture supports policy-based access control, local processing, and purpose-limited disclosure for sensing requests handled by the network. Although the work does not focus on physiological sensing, it is particularly relevant at L3 because physiological or biometric sensing requires strict control over what is collected, where it is processed, and which applications may access the resulting information.

6 Research Roadmap

The preceding sections show that privacy in ISAC concerns the collection, processing, inference, storage, and disclosure of sensing-derived information about active users, UEs, bystanders, passive objects, and environments. Based on the sensing-data levels in Section 2.3, the applications in Section 3, the privacy challenges in Section 4, and the solution directions in Section 5, the following research directions are central for privacy-preserving ISAC.

1. **Privacy-by-design for sensing signals and sensing capabilities.** Future ISAC systems require designs in which privacy leakage is considered together with communication rate, sensing accuracy, latency, and energy consumption. Key open problems are to define privacy metrics for the sensing-data levels L1-L3, adapt waveforms and beams to the sensing resolution required by each service, and limit unauthorized sensing.
2. **Location and environment privacy under high-resolution sensing.** Location and environment data form the first privacy-sensitive layer of ISAC. Future work must protect active users, bystanders, passive objects, and environments in the sensing area. Important directions include pseudolocation, location obfuscation, privacy-aware beam and access-point selection, and service-level rules that avoid unnecessary location precision.
3. **Data minimization and privacy-preserving sensing pipelines.** Privacy protection should be integrated before raw CSI, radar, and localization data are stored, transferred, or disclosed. Open problems include identifying application-specific minimal sensing features, separating raw measurements from application-facing results, enforcing retention limits, and combining anonymization, pseudonymization, encryption, and access control in ISAC functions.
4. **Protection against behavioral and physiological inference.** Behavioral and physiological sensing correspond to the more privacy-sensitive levels L2 and L3. Future ISAC research must limit unnecessary behavioral and physiological inference while preserving the intended sensing service. Key directions include feature sanitization for CSI and radar data, privacy-preserving activity recognition, and privacy-aware handling of biometric or health-related sensing results.
5. **Consent, transparency, data ownership, and accountability.** Technical privacy mechanisms must be supported by governance mechanisms for sensing requests and sensing results. Future architectures need explicit sensing policies, consent management, transparency logs, and fine-grained authorization. Open problems include data ownership for bystander sensing, permission revocation, third-party auditing, and measurable privacy criteria for system design.

These directions are interdependent. Physical-layer mechanisms influence what can be sensed, data-minimization mechanisms influence what is stored or shared, learning-based pipelines influence what can be inferred, and governance mechanisms determine who may request, process, and disclose sensing

results. Addressing these aspects together is necessary for ISAC systems that provide useful sensing services while respecting privacy expectations and legal requirements.

7 Conclusion

In this work, we discussed privacy challenges and solution directions for next-generation ISAC systems. We focused on privacy issues caused by sensing-derived information, rather than the confidentiality of communication content. In particular, we emphasized that ISAC can affect not only active users and their UEs, but also bystanders, passive objects, and the surrounding environment. To organize these risks, we classified privacy-sensitive sensing data into three levels: location and environment data, behavioral data, and physiological data. This classification was then used to relate sensing capabilities and applications to privacy concerns.

We summarized representative internal and external ISAC applications and showed that their privacy impact depends on the type and granularity of the sensing data they require. We then reviewed privacy challenges related to consent, transparency, data ownership, profiling, location tracking, behavioral inference, and physiological sensing. Representative solution directions were discussed, including control of spatial observability, location obfuscation, AN-based protection, RIS-based privacy approaches, directional sensing constraints, privacy-aware system architectures, and privacy-preserving feature extraction mechanisms.

Finally, we outlined a research roadmap for privacy-preserving ISAC. The main open directions include privacy-by-design for sensing signals and sensing capabilities, location and environment privacy under high-resolution sensing, data minimization in sensing pipelines, protection against unnecessary behavioral and physiological inference, and governance mechanisms for consent, transparency, ownership, and accountability. Addressing these directions together is necessary for future ISAC systems that provide useful sensing services while respecting privacy expectations and legal requirements.

Acknowledgments. The work of O. Günlü was partially supported by the ZENITH Research and Leadership Career Development Fund under Grant ID23.01, EU COST Action 6G-PHYSEC, Swedish Foundation for Strategic Research (SSF) under Grant ID24-0087, and German Federal Ministry of Research, Technology and Space (BMFTR) 6GEM+ Transfer Hub under Grants 16KIS2412 and 16KISS005. The work of P. Dass is financed based on the budget passed by the Saxonian State Parliament in Germany. The work of J.P. Vilela is funded by national funds through FCT – Fundação para a Ciência e a Tecnologia, I.P., under the support UID/50014/2025 (`https://doi.org/10.54499/UID/50014/2025`).

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. 3GPP: Feasibility Study on Integrated Sensing and Communication (Release 19). Tech. Rep. TR 22.837 V19.4.0, 3GPP Technical Specification Group TSG SA (2024)
2. Adib, F., Katabi, D.: See through walls with WiFi! In: ACM SIGCOMM. pp. 75–86 (2013)
3. Aldirmaz-Colak, S., et al.: A comprehensive review on ISAC for 6G: Enabling technologies, security, and AI/ML perspectives. IEEE Access **13**, 97152–97193 (2025)
4. Bartoletti, S., et al.: Security and privacy for ISAC. In: Caire, G. (ed.) Integrated sensing and communications. Texmat (2025)
5. Bergström, D., Günlü, O.: Deep randomized distributed function computation (DeepRDFC): Neural distributed channel simulation. In: IEEE International Symposium on Information Theory (ISIT). pp. 1–6 (2025)
6. Cigno, R.L., Gringoli, F., Cominelli, M., Ghiro, L.: Integrating CSI sensing in wireless networks: Challenges to privacy and countermeasures. IEEE Network **36**(4), 174–180 (2022)
7. Cunha, M., Mendes, R., de Montjoye, Y.A., Vilela, J.P.: Compromising location privacy through Wi-Fi RSSI tracking. Nature Scientific Reports **15**(1) (2025)
8. Dass, P., Ujjwal, S., Novotny, J., Zolotavkin, Y., Laaroussi, Z., Köpsell, S.: Addressing privacy concerns in joint communication and sensing for 6G networks: Challenges and prospects. In: Annual Privacy Forum. pp. 87–111. Springer (2024)
9. Dass, P., Zolotavkin, Y., Köpsell, S.: Privacy preserving integrated sensing and communication architecture for 6g networks. In: Sargento, S., Saeed, A., Kolios, P., Dovrolis, C., Vassiliou, V. (eds.) 2025 IFIP Networking Conference, Limassol, Cyprus, 26-30 May 2025. IFIP Open Digital Library (2025), `https://opendl.ifip-tc6.org/db/conf/networking/networking2025/1571141814.pdf`
10. Dass, P., Zolotavkin, Y., Köpsell, S., Sen, P.: An architectural approach to security and privacy in isac-enabled user equipment. In: IEEE Middle East Conference on Communications and Networking (MECOM). pp. 1–6 (2025)
11. De Lima, C., et al.: Convergent communication, sensing and localization in 6G systems: An overview of technologies, opportunities and challenges. IEEE Access **9**, 26902–26925 (2021)
12. Delgado-Santos, P., Tolosana, R., Guest, R., Vera-Rodriguez, R., Deravi, F., Morales, A.: GaitPrivacyON: Privacy-preserving mobile gait biometrics using unsupervised learning. Pattern Recognition Letters **161**, 30–37 (2022), `https://www.sciencedirect.com/science/article/pii/S0167865522002264`
13. Deng, M., Wuyts, K., Scandariato, R., Preneel, B., Joosen, W.: A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requirements Engineering **16**(1), 3–32 (2011)
14. Droulias, S., Stratidakis, G., Alexiou, A.: Bending beams for 6G near-field communications. IEEE Transactions on Wireless Communications (TWC) **24**(2), 1467–1480 (2025)
15. Du, R., et al.: An overview on IEEE 802.11 bf: WLAN sensing. IEEE Communications Surveys & Tutorials (COMST) (2025)
16. ETSI: Integrated Sensing And Communications (ISAC); Security, Privacy, Trustworthiness and Sustainability. Tech. Rep. GR ISC 004 V1.1.1 (2026-02), ETSI (2026)
17. European Parliament, Council of the European Union: Regulation (EU) 2016/679 of the European Parliament and of the Council, `https://data.europa.eu/eli/reg/2016/679/oj`

18. Gao, F., Xu, L., Ma, S.: Integrated sensing and communications with joint beam-squint and beam-split for mmWave/THz Massive MIMO. IEEE Transactions on Communications (TCOM) **71**(5), 2963–2976 (2023)
19. González-Prelcic, N., et al.: The integrated sensing and communication revolution for 6G: Vision, techniques, and applications. Proceedings of the IEEE **112**(7), 676–723 (2024)
20. Günlü, O.: Randomized distributed function computation (RDFC): ultra-efficient semantic communication applications to privacy. Springer Journal on Information Security (JIS) (2026)
21. Günlü, O., Bloch, M., Schaefer, R.F.: Private remote sources for secure multi-function computation. IEEE Transactions on Information Theory (T-IT) **68**(10), 6826–6841 (2022)
22. Günlü, O., Bloch, M.R., Schaefer, R.F., Yener, A.: Secure integrated sensing and communication. IEEE Journal on Selected Areas in Information Theory (JSAIT) **4**, 40–53 (2023)
23. Illi, E., et al.: Physical layer security for authentication, confidentiality, and malicious node detection: A paradigm shift in securing IoT networks. IEEE Communications Surveys & Tutorials (COMST) **26**(1), 347–388 (2024)
24. International Telecommunication Union: Framework and Overall Objectives of the Future Development of IMT for 2030 and Beyond. ITU-D SG2 Q3/2 Workshop on 5G Cybersecurity, presentation slides (May 2024), `https://www.itu.int/dms_pub/itu-d/oth/07/31/D07310000090015PDFE.pdf`, accessed: 2026-05-15
25. Isaia, C., Michaelides, M.P.: A review of wireless positioning techniques and technologies: From smart sensors to 6G. Signals **4**(1), 90–136 (2023)
26. Keskin, M.F., et al.: Multi-domain security for 6G ISAC: Challenges and opportunities in transportation. arXiv preprint arXiv:2511.16316 (2025)
27. Keya, M., Zu, X., Yuan, J., He, Y., Zeng, K., Jiao, L.: Fine-grained location privacy protection in 6G ISAC systems using deep learning. In: IEEE Military Communications Conference (MILCOM). pp. 627–632 (2024)
28. Khan, M.A.A.H., et al.: RAM: Radar-based activity monitor. In: IEEE INFOCOM 2016-IEEE International Conference on Computer Communications. pp. 1–9 (2016)
29. Khan, U.A., Ho, L., Claussen, H., Flanagan, M.F., Kundu, C.: On beamforming for transmitter location privacy in MIMO systems. arXiv preprint arXiv:2508.09882 (2025)
30. Li, C., Liu, M., Cao, Z.: WiHF: Gesture and user recognition with WiFi. IEEE Transactions on Mobile Computing (TMC) **21**(2), 757–768 (2022)
31. Li, Y., et al.: RIS-based physical layer security for integrated sensing and communication: A comprehensive survey. IEEE Internet of Things Journal (IoTJ) **12**(16), 32444–32468 (2025)
32. Liu, F., Cui, Y., Masouros, C., Xu, J., Han, T.X., Eldar, Y.C., Buzzi, S.: Integrated sensing and communications: Toward dual-functional wireless networks for 6G and beyond. IEEE Journal on Selected Areas in Communications (JSAC) **40**(6), 1728–1767 (2022)
33. Liu, F., Masouros, C., Petropulu, A.P., Griffiths, H., Hanzo, L.: Joint radar and communication design: Applications, state-of-the-art, and the road ahead. IEEE Transactions on Communications (TCOM) **68**(6), 3834–3862 (2020)
34. Liu, R., et al.: Secure communications, sensing, and computing toward next-generation networks. IEEE Journal on Selected Areas in Communications (JSAC) **44**, 4444–4470 (2026)

35. Liu, T., et al.: 6G integrated sensing and communications channel modeling: Challenges and opportunities. IEEE Vehicular Technology Magazine (VTMAG) **19**(2), 31–40 (2024)
36. Ma, T., Xiao, Y., Lei, X., Xiao, M.: Sensing - resistance-oriented beamforming for privacy protection from isac devices. In: IEEE International Conference on Communications Workshops (ICC Workshops). pp. 1207–1212 (2024)
37. Ma, Y., Zhou, G., Wang, S., Zhao, H., Jung, W.: SignFi: Sign language recognition using WiFi. ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT) **2**(1) (2018)
38. Magbool, A., Kumar, V., Renzo, M.D., Flanagan, M.F.: Hiding in plain sight: RIS-aided target obfuscation in ISAC. IEEE Transactions on Wireless Communications (TWC) **25**, 14550–14563 (2026)
39. Martins, Ó., Vilela, J.P., Gomes, M.: WiFi-based person identification through motion analysis. In: IEEE International Mediterranean Conference on Communications and Networking (MeditCom) (2024)
40. Martins, Ó.G., et al.: Delving into security and privacy of joint communication and sensing: A survey. IEEE Open Journal of the Communications Society (OJCOM) (2025)
41. Matsumine, T., Ochiai, H., Shikata, J.: Physical layer security for integrated sensing and communication: A survey. IEEE Open Journal of the Communications Society (OJCOM) **6**, 6690–6743 (2025)
42. Meneghello, F., Garlisi, D., Fabbro, N.D., Tinnirello, I., Rossi, M.: Sharp: Environment and person independent activity recognition with commodity IEEE 802.11 access points. IEEE Transactions on Mobile Computing (TCM) **22**(10), 6160–6175 (2023)
43. Naeem, F., Ali, M., Kaddoum, G., Huang, C., Yuen, C.: Security and privacy for reconfigurable intelligent surface in 6g: A review of prospective applications and challenges. IEEE Open Journal of the Communications Society **4**, 1196–1217 (2023)
44. Nguyen, V.L., Hwang, R.H., Cheng, B.C., Lin, Y.D., Duong, T.Q.: Understanding privacy risks of high-accuracy radio positioning and sensing in wireless networks. IEEE Communications Magazine (COMMAG) **62**(5), 104–111 (2024)
45. Okano, T., Izumi, S., Kawaguchi, H., Yoshimoto, M.: Non-contact biometric identification and authentication using microwave Doppler sensor. In: IEEE Biomedical Circuits and Systems Conference (BioCAS). pp. 1–4 (2017)
46. Qu, K., Ye, J., Li, X., Guo, S.: Privacy and security in ubiquitous integrated sensing and communication: Threats, challenges and future directions. IEEE Internet of Things Magazine (IoTMAG) **7**(4), 52–58 (2024)
47. Qu, Y., Zhang, Y., Wang, Y., Yang, Y.: Secure and privacy-preserving issues in integrated sensing and communication-enabled wireless networks: a survey. EURASIP Journal on Advances in Signal Processing **2026**(1), 4 (2026)
48. Ratnam, V.V., Chen, H., Chang, H.H., Sehgal, A., Zhang, J.: Optimal preprocessing of WiFi CSI for sensing applications. IEEE Transactions on Wireless Communications (TWC) **23**(9), 10820–10833 (2024)
49. Sobron, I., Del Ser, J., Eizmendi, I., Vélez, M.: Device-free people counting in IoT environments: New insights, results, and open challenges. IEEE Internet of Things Journal (IoTJ) **5**(6), 4396–4408 (2018)
50. Stratidakis, G., Droulias, S., Alexiou, A.: Perceptive, resilient, and efficient networks: Programming the wireless environment with reconfigurable intelligent surfaces. IEEE Vehicular Technology Magazine (VTMAG) **19**(4), 36–43 (2024)

51. Stratidakis, G., Droulias, S., Alexiou, A.: Near-field hierarchical localization for integrated sensing and communication. IEEE Access **13**, 17766–17776 (2025)
52. Su, N., et al.: Integrating sensing and communications in 6G? Not until it is secure to do so. arXiv preprint arXiv:2503.15243 (2025)
53. Sun, Y., Liu, J., Wang, J., Cao, Y., Kato, N.: When machine learning meets privacy in 6G: A survey. IEEE Communications Surveys & Tutorials (COMST) **22**(4), 2694–2724 (2020)
54. Suzuki, H., et al.: Security and privacy in 6G mobile (2025), `https://www.csiro.au/-/media/D61/Reports/6G-report/SecurityandPrivacyin6GMobileReport.pdf`
55. Tahmoush, D.: Review of micro-Doppler signatures. IET Radar, Sonar & Navigation **9**(9), 1140–1146 (2015)
56. Wang, W., Liu, A.X., Shahzad, M.: Gait recognition using WiFi signals. In: ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp). p. 363–373 (2016)
57. Wei, Z., Liu, F., Masouros, C., Su, N., Petropulu, A.P.: Toward multi-functional 6G wireless networks: Integrating sensing, communication, and security. IEEE Communications Magazine (COMMAG) **60**(4), 65–71 (2022)
58. Welling, T., Günlü, O., Yener, A.: Secure integrated sensing and communication: Information theory offers insights. arXiv preprint arXiv:2605.08106 (2026)
59. Wu, K., Wang, Z., Chen, S.L., Zhang, J.A., Guo, Y.J.: ISAC: From human to environmental sensing. IEEE Journal of Selected Topics in Electromagnetics, Antennas and Propagation (JSTEAP) **1**(1), 84–98 (2025)
60. Wu, N., Jiang, R., Wang, X., Yang, L., Zhang, K., Yi, W., Nallanathan, A.: AI-enhanced integrated sensing and communications: Advancements, challenges, and prospects. IEEE Communications Magazine (COMMAG) **62**(9), 144–150 (2024)
61. Xue, X., Parkar, S., Yu, S., Zheng, Y.: AI-assisted composite ISAC for mmWave respiration pattern recognition. In: IEEE Annual Congress on Artificial Intelligence of Things (AIoT). pp. 357–364 (2025)
62. Yadav, S.K., et al.: CSITime: Privacy-preserving human activity recognition using WiFi channel state information. Elsevier Neural Networks **146**, 11–21 (2022)
63. Zhang, D., et al.: Integrated sensing and communications over the years: An evolution perspective. IEEE Communications Surveys & Tutorials (COMST) **28**, 5014–5048 (2026)
64. Zhang, J.A., et al.: An overview of signal processing techniques for joint communication and radar sensing. IEEE Journal of Selected Topics in Signal Processing (JSTSP) **15**(6), 1295–1315 (2021)
65. Zhang, J.A., et al.: Enabling joint communication and radar sensing in mobile networks - A survey. IEEE Communications Surveys & Tutorials (COMST) **24**(1), 306–345 (2022)
66. Zhang, L., Cui, W., Li, B., Chen, Z., Wu, M., Gee, T.S.: Privacy-preserving cross-environment human activity recognition. IEEE Transactions on Cybernetics **53**(3), 1765–1775 (2023)
67. Zhang, R., He, Y., Yuan, L., Li, Z., He, C., Tan, F.: Empowering 6G ambient intelligence with Terahertz integrated sensing and communications. IEEE Wireless Communications **31**(5), 256–263 (2024)
68. Zhao, X., Zhang, D., Yin, H., Mao, D., Li, H.: Remote vital sign monitoring based millimeter-wave sensing. IEEE Access **12**, 142760–142771 (2024)
69. Zhou, B., et al.: 6G ISAC enables environment object reconstruction. IEEE Journal of Selected Topics in Electromagnetics, Antennas and Propagation (JSTEAP) **1**(1), 165–178 (2025)

70. Zhu, X., Liu, J., Lu, L., Zhang, T., Qiu, T., Wang, C., Liu, Y.: Enabling intelligent connectivity: A survey of secure ISAC in 6G networks. IEEE Communications Surveys & Tutorials (COMST) **27**(2), 748–781 (2025)
71. Zou, J., Masouros, C., Liu, F., Sun, S.: Securing the sensing functionality in ISAC networks: An artificial noise design. IEEE Transactions on Vehicular Technology (TVT) **73**(11), 17800–17805 (2024)