Open6GHub

JCAS and Privacy

Position Paper

Open6GHub
July 2024
V1.0

Outline

SPONSORED BY THE

Federal Ministry
of Education
and Research

The work presented is part of the BMBF project “Open6GHub”. The views expressed herein can in no way be taken to reflect the official opinion of the BMBF.

Authors

Torsten Reissland (FAU Erlangen-Nürnberg), Tobias Jung (FAU Erlangen-Nürnberg), Fabian Eichhorn (Fraunhofer FOKUS), Marius Corici (Fraunhofer FOKUS), Atta Ullah (RPTU), Benjamin Nuss (KIT), Julian Todt (KIT), Thorsten Strufe (KIT), Lukas Brechtel (DFKI), Christof Rauber (DFKI), Norman Franchi (FAU Erlangen-Nürnberg), Hans D. Schotten (DFKI, RPTU), Reiner Thomä (TU Ilmenau)

Introduction

The term Joint Communication and Sensing (JCAS) refers to techniques which use the radio communication infrastructure and possibly also the signals for the purpose of sensing. In this work we focus more specifically on radar and spectrum sensing. Radar sensing refers to the sensing of various properties of physical objects. First and foremost, these properties include position and movement, where the latter includes the velocity and acceleration of the overall object as well as phenomena like vibrations or other micro movements. Moreover, classification of objects and identification of individual objects are known applications of radar systems.

However, the term sensing can be broadened to radio sensing for spatial electromagnetic (EM) analysis, which we call 'spectrum sensing' in the following for brevity reasons. An ever-growing number of wireless devices increases interference and radio resource management difficulties. Spectrum sensing can address these issues, facilitating transmitter detection, localization, and signal classification in the area of interest. Furthermore, building an accurate digital twin of the EM environment can be seen as an ultimate goal. This is achievable via real-time automated distributed spectrum sensing, which can be implemented as several sensing units (SUs) constantly scanning the same environment from different perspectives.

JCAS can be used in conjunction with very different types of communication systems. For example, the standard IEEE 802.11bf already enables the widespread adoption of WLAN sensing [1]. In a very broad sense, also passive radar systems could be classified as JCAS technology, as they make use of broadcast communication signals. However, this paper focuses on public mobile communication networks of the next generation. This focus limits the considered bands to the already adopted FR1 and FR2 bands with a current maximum bandwidth of 400 MHz. Campus networks, even though they are technically very similar, are excluded from the discussion here, as the use in private areas leads to deviating legal implications.

JCAS, in the mentioned context offers the possibility to integrate additional features into the mobile communication infrastructure. As hardware and spectrum can be shared between sensing and communication applications, this allows to implement these features with reduced cost and a more efficient use of spectrum, compared to standalone sensing systems. Furthermore, such a JCAS system works more robust in difficult environmental conditions, compared to optical systems. However, the potential widespread adoption of JCAS in the mobile communication infrastructure also raises the question of possible privacy issues for people in monitored areas. This question, alongside its legal implications will be discussed in this paper. For this, first some terminology on privacy will be established, before a more thorough introduction on use cases for JCAS is presented. Next, a possible services architecture for JCAS is proposed before some privacy concerns are illustrated. Based on that, legal implications and countermeasure for these concerns are presented before the paper is concluded.

Background on Privacy

Especially in the context of culturally and juridically nuanced terminology, definitions, such as privacy, need to be precise. As this paper is authored by a European research group, terms are defined according to European cultural understanding and applicable EU laws and regulations. Internationally, privacy encompasses the "right to be left alone," meaning freedom from any kind of interference, as articulated in Article 12 of the Universal Declaration of Human Rights. Consequently, every individual has the right to informational self-determination, allowing each person to decide how their personal data is handled. This implies that processing of personally identifiable information requires a legal basis, either fulfilment of a contract with the individual, or a clear and informed consent (opt-in). These two fundamental definitions build the core of the European definition of privacy. Personal data in this sense refers to any information that can be linked to a natural person. An example of this would be a name or passport number. There is also a weaker version of personal data, non-sensitive data, that can only indirectly be linked to a natural person. This is for example location data, IP-addresses, or rough movement behaviour. This data can be directly identifying, or at least combining multiple such data types and/or by creating a likely link to sensitive personal data will allow to uniquely identify a natural person.

The technical and organizational actions and measures required to protect all kinds of personal data and to ensure privacy are defined as data protection. In the EU, the obligations of protecting personal data of natural persons are enshrined in the GDPR. When the requirements are technical in nature, the implementation of protective measures is defined as data security. Since this paper discusses JCAS in public telecommunication infrastructure, it is important to note that, according to Article 95 of the GDPR, the telecommunications industry in the EU is also regulated by the ePrivacy Directive (Directive 2002/58/EC), which specifies the conditions under which data can be processed without falling under restrictions of the GDPR. Understand, also that processing in the sense of the GDPR is more holistic than in the technical terminology. Therefore, even the collection and gathering of data that has a possibility to cause privacy concerns already falls under the GDPR, even if further “processing” is necessary in a technical sense.

To gain further understanding in which cases the ePrivacy Directive substitutes the GDPR, the ePrivacy Directive needs to be examined in detail. In the articles 6 and 9, the ePrivacy Directive allows telecommunication service providers processing of certain data types collected from its *subscribers and users*. Article 2 follows up with a definition of “users”, explaining that any natural person using a publicly available electronic communication service is defined as a user. An interpretation of this would be that as long as one has a turned-on smartphone with a SIM-card, assuming airplane mode is turned off, one counts as a user to all mobile telecommunication networks. Two relevant data types mentioned in the ePrivacy Directive are traffic and localization data, which can be considered the same data type as JCAS data. The distinction between these two is whether the data is used to increase the performance of electronic communication, or if it is offered as a “value added service” to subscribers and users, that is clearly stated in the contracts with the users. For traffic data no further consent is needed for the processing of telecommunication service providers aside from being a user or subscriber, see article 6. A processing of localization data on the other hand, especially if offered through value added services, has stricter privacy requirements, such as the necessity of consent, and the right to retract the consent.

Given the significance and applicability of both the GDPR and the ePrivacy Directive for JCAS services offered by telecommunication providers, relevant articles and recitals will be examined to ensure our understanding and compliance of JCAS with EU and international laws and regulations. The implications of the introduced laws and their content will be discussed extensively in sections about privacy concerns and privacy measures.

Lastly, our understanding of the processes of anonymization and pseudonymization, which are concepts to increase or achieve privacy, are explained. Both are referenced by the GDPR and the ePrivacy Directive. Anonymization has the goal of preventing any linking to natural persons in any data. The resulting dataset possesses no means of any reciprocal mechanism which can revert it back into or link it to the original personal data. In other words, if there is a way to retroactively retrieve or link it to personal data, then it is not successfully anonymized. For clarification consider the following: Assuming a list of customer names and purchased products. To remove a possible identification, we need to replace the names with random identifiers and remove any linkability to place, time or other records and mechanism of the products purchased. Additionally, it must be noted that the identified personal data cannot be captured, or at least needs to be deleted. The advantage of anonymized data is that it removes the applicability of the GDP, see recital 26, and the necessity of deletion of personal data, as is often required by the ePrivacy Directive. Because of the removed linkability, successfully anonymized can be used, and traded with third parties, without any restriction by either of these laws. Measures with which anonymization and pseudonymization can be achieved are found in [2] [3].

Pseudonymization just as anonymization replaces personal data through artificial and sometimes temporary identifiers or attributes. The goal is, again, to prevent linkability of personal data to natural persons. However, in contrast to anonymization, the process can be reversible and the datasets themselves remain linkable. The data or information needed to reverse the pseudonymization need to be prevented or strictly protected by data security measures. It follows that, in general, pseudonymized data increases the effort and complexity necessary to identify a natural person. Therefore, it counts as a privacy enhancing measure, which is encouraged by both the GDPR and ePrivacy Directive. Possible implementations of these concepts will be discussed in the later section.

Vision on Joint Communication and Sensing

To understand the deeper motivation behind the research into JCAS in mobile communications, some examples from Open6GHub’s vision on the applications of a JCAS system are introduced.

As a result of climate change, increasingly large amounts of rain are falling in small areas over short periods of time. This leads to flooding, even in places that were previously considered safe. People are unknowingly put at risk when roads are suddenly flooded. Cameras and sensors are already being used in potential flood zones. However, the changing rainfall patterns caused by climate change are making it increasingly difficult to accurately predict flood hazards. However, radio waves can be used to effectively detect floods. This technology enables rapid and reliable hazard assessment and can thus save lives.

But even in less severe situations, the attenuation effects of raindrops on radio transmissions can be taken advantage of. In the agricultural sector for example, rainfall monitoring is important for crop irrigation management but also for the general study and scientific observation of the climate. Using base stations to detect and measure rainfall can allow covering large areas without the need to install and maintain rain gauges in numerous locations. This can provide immediate feedback on rainfall to 6G users, but also continuously monitor precipitation rates for statistical analysis and evaluation. A weather service could use the measurement data in combination with other factors such as wind speed and direction to predict the short-term path of the rain and inform users in those locations via push-notifications or short messages.

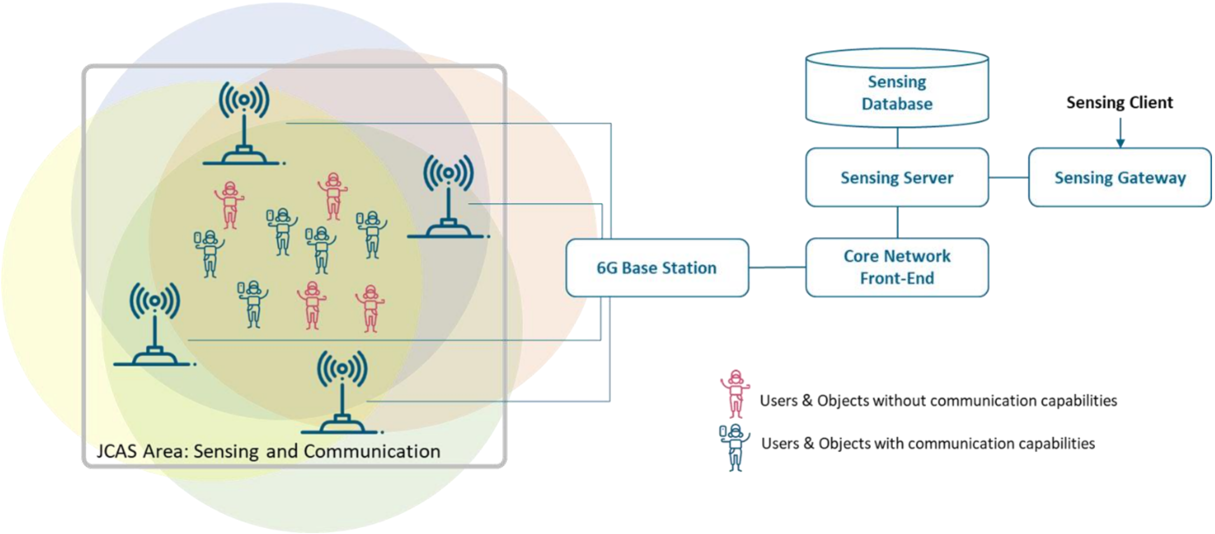
Crowd management is an important task in the planning and execution of large public events. The main goal is to avoid critical densities of people in the prevention of mass panics. One useful tool during such an event is a monitoring system which either counts people at passing points or estimates the number of people in a given area. Nowadays camera solutions are employed for such tasks, but JCAS systems working in the FR2 band could solve this task with lower hardware efforts. This solution might also reduce some costs as already installed base stations can be utilized for this task.

The surveillance of parking lots in public spaces enables improvements in the utilization of public space and in traffic flow control. This is done by providing drivers with information about available places. At the moment, also for this task, mostly cameras are employed. Of course, such an approach could be extended towards general traffic monitoring.

Monitoring railway crossings with cameras is one way to prevent fatal accidents, as a train can be warned in time, if an object or person is detected on the tracks. Using JCAS instead, would offer the advantage that the mobile communication infrastructure along the tracks can be used to not only monitor the train crossing but also other parts of the train tracks to avoid, for example, collisions with animals. Therefore, cost for hardware could be reduced.

Some of the mentioned use cases can only be addressed by a JCAS or a radar system, while others could also be addressed by other sensing technologies, such as cameras. In any case, employing a JCAS system, obviously has some implications on the privacy of people in a surveilled area. Considering the importance of privacy for public acceptance of any technology and compliance with legal norms, a critical assessment of these implications is necessary. Therefore, the advantages and challenges of utilizing JCAS in critical areas are to be assessed in this paper.

JCAS Service Architecture


Sensing Database
Sensing Client
Sensing Server
Sensing Gateway
6G Base Station
Core Network Front-End
JCAS Area: Sensing and Communication
Users & Objects without communication capabilities
Users & Objects with communication capabilities

While most Joint Communication and Sensing (JCAS) work has focused on developing technology that uses signals to assess environmental properties, there is a noticeable gap in the literature regarding services that could leverage these signals. In 6G networks, we foresee that communication will still function across the RAN and core network, following a similar pattern, but the sensing aspect requires a new service architectural approach that should include basic principles such as privacy-by-design. Minimizing privacy sensitive data traffic and exposure, while at the same time keeping the data under high data security protection measures.

Sensing shifts the focus from a user-targeted service to an area-based service, working within specific geographic regions where the RAN supports JCAS, independent of user identities, even if they can communicate. This change alters the service identification from the typical user identifier, which has long been a staple in telecom, to an area identifier. Existing identifiers, such as tracking areas, can be re-engineered to define these regions, but they must adapt to smaller JCAS zones. Although large JCAS regions might be feasible, they are often smaller than traditional tracking areas, and privacy considerations might call for dividing them into even smaller parts.

To process the information from JCAS-capable RANs, a sensing service collects data from various radio heads and base stations, regularly, event-based or on demand. The raw signals may come from many sources, but the processed data is more manageable as being area based. Given consent of the sensed individuals - or another legal basis for processing - this data is sent to a sensing server, which derives secondary information, (like counting people in a specific location), and stores it in a sensing database. The derived information can also be supplemented with mobility patterns from connected devices or location services to enhance user monitoring and sensing.

For external access, a sensing service client sends requests to a gateway, which checks credentials to ensure proper authorization to access the data for a specific area. The gateway retrieves the requested information from the database or triggers the sensing service to initiate new operations to collect data. This system's design is similar to the current location services in 5G, adapted for 6G. While 5G relies on the Access and Mobility Function (AMF) as the front-end for RAN messages, the 6G equivalent should be a more flexible front-end function that routes requests to the appropriate service without fully decoding them.

Please note that we presented just an initial architecture outline. Further design work is needed to address protocol selection, procedural steps, and operational considerations, including reliability, quality of the sensing service in regard to mis-sensings, security, resource consumption, and energy efficiency.

Privacy concerns

Note, that JCAS can indeed provide privacy benefits: Given a setup in which premises are observed with visual light video or thermal imaging and a legal basis for processing, deploying JCAS instead may allow for similar functionality while actually processing less rich data of individuals.

Despite such benefits offered by JCAS-based applications, they also raise privacy concerns in other scenarios. The extensive data collection facilitated by sensors, coupled with the integration of location data and other information, poses risks to privacy. This is further exacerbated by the risk of system compromise through malicious actors.

JCAS inherently is a sensing technology that allows to identify passers-by and may allow for inference of personal attributes. All data captured with JCAS hence has to be considered personal data and any processing is subject to regulation, like, for instance in Europe, the GDPR.

In principle it is possible to record human speech using radio signals. An example for this is presented in [4]. However, as this system operates at 160 GHz and requires physical contact to the speaker, it does not prove JCAS systems to be a privacy threat in this regard. In contrast to this, [5] presents a MIMO system operating at 60 GHz with a bandwidth of 1.5 GHz. This frequency and bandwidth are covered by the highest frequencies in the FR2 range. The limiting factor of this system is its range of only 2.5 m. Still, as similar JCAS featured mobile communication systems are possible, this scenario has to be taken into account regarding privacy concerns. A similar system operating between 76 GHz and 81 GHz is able to detect speech even from vibrations of objects close to the speaker, i.e. without line of sight [6]. However, this system was only tested at a range of 0.5 m at most with a thin barrier. Therefore, it won’t be applicable in cellular networks. Furthermore, it can be summarized that such speech recognitions were only achieved in the V-band or at even higher frequencies. Therefore, it can be presumed that currently used systems do not collect any speech information, regardless of the actual processing steps.

JCAS is essentially a sensing technology like visual light imaging, which introduces sensors that collect reflections within a spectrum of electromagnetic waves on a large scale. Much alike video processing, it enables real-time gathering of personal data, and hence tracking of individuals. It also allows for the inference of additional personal attributes, like activities, ticks, medical conditions, and a variety of biometric measures. This obviously raises concerns regarding the misuse of such data, and privacy threats that arise. Consequently, since this data cannot be considered anonymous, it causes the applicability of privacy regulations such as the GDPR.

By combining personal data gained from JCAS with widely publicly accessible information, exemplary such from social media or webpages, it will be possible to create an everyday behaviour profile of natural persons. In theory this is already possible with one or a combination of multiple surveillance system. But the increased range, angle, and mass of JCAS data gathering allows for surveillance of a much larger area. On top of that JCAS may allow gathering massive amounts of information that is comparable to information that can normally only be achieved through a combination of multiple sophisticated surveillance techniques. Again, it should be noted that surveillance related activities such as tracking are already possible through techniques such as smartphone-based GPS-Tracking or identifiers in cellular networks [7]. In the same sense speech monitoring through a smart phone’s microphone is also already possible. General activity over the Wi-Fi home network is possible through internet service providers or Wi-Fi channel spectrum observations [8]. Any outdoor activity, for example driving in a car can be monitored through street cameras, GPS, sensory systems of cars or other city infrastructure [9]. As a result, widespread surveillance is already possible *right now* by using these different techniques and datasets. The concern regarding JCAS is that its surveillance capacity is as powerful as the surveillance of multiple of these techniques combined and therefore replace those through a singular technology which would drastically reduce complexity and effort. The almost ubiquitous coverage that mobile service providers have exacerbates this concern. The emergent problem arriving from this is that, through drastically reduced effort, surveillance will become available for more people while simultaneously less power and resources are required. Therefore, regulations on usage and implementation of JCAS need to be discussed earlier rather than later.

Unlike current localization methods of the telecommunications industry, JCAS also affects persons who are not considered user or subscribers which is stated and covered in the ePrivacy Directive. Consequently, in this case such natural persons do then primarily fall under the regulations of the GDPR instead. Furthermore, as explained in the privacy background section, there are different data types defined in the ePrivacy Directive. On the one hand if JCAS data is used to improve or optimize the steering of user data, localization data gathered through JCAS falls under traffic data regulations. On the other hand, if it is sold to subscribers and users or third parties, it falls under a value-added service. The application of these regulations relating to JCAS data is shown graphically in Figure 2.

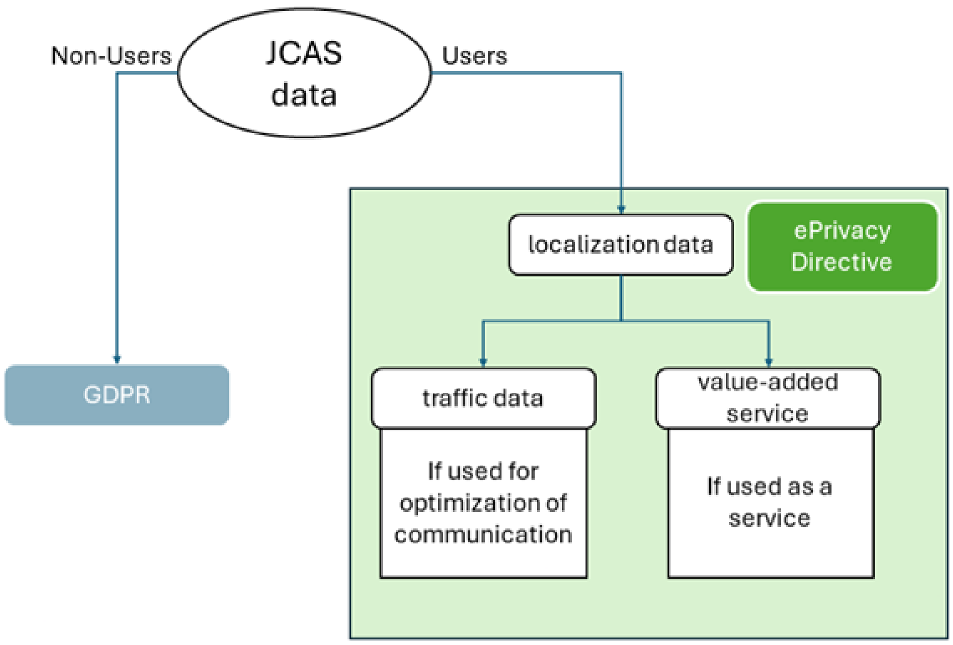


Figure 2: Applicability of JCAS data to European regulations depending on data usage and customers of consumed services.

In each of these cases shown in Figure 2 the applied laws and relevant articles, name slightly different requirements from a legal perspective. It follows that an implementation from a technical perspective would also be more complex due to the differences of requirements and necessity of classifying datasets case to case. While this does not affect privacy directly, unclear legislation and requirements does affect the implementation of data protection and data security measures which in turn do affect privacy.

Privacy and Security Measures

JCAS unquestionably has a weakened linkability when comparing the captured data with, for instance, visible-light or thermal imaging. Still, the collected data can be attributed to individuals and better understanding of the inherent threats and venues towards either anonymizing or finding other ways of protection is direly needed. To address the aforementioned privacy concerns of the last chapter, ensure data protection and compliance to EU regulations, several measures will be discussed.

JCAS services which are offered by telecommunication service providers and offered to non-users fall under the GDPR. In the same sense, JCAS data gathered from users, from the viewpoint of the ePrivacy Directive, can either be traffic data or a “value added service”.As our foremost measure to ensure data security and privacy of JCAS we propose drawing a more specific jurisdiction between the GDPR and ePrivacy Directive for JCAS data, whether used for optimization in communication systems or as a service. Hereby the goal is to clarify the legal requirements and gives a stringent guideline for data protection measures necessary and recommended to enhance privacy.

Our focus from here onwards will be on technical measures and implementations to increase privacy and data protection. Of course, next to these, other requirements of the GDPR and ePrivacy Directive are also important. Such requirements would for example include a clear responsibility and contact for privacy issues, high data security of processed data, transparency of data processing through audits or certificates, and insurance of the accuracy of given data.

Anonymization Measures

As explained in the chapter "background to privacy", anonymization is a powerful tool to ensure privacy. As stated in recital 26 of the GDPR and articles 6, 9 of the ePrivacy Directive as well as in recitals 9, 26 and 28 of the same. In these paragraphs the power of anonymization is often put equally to a deletion of the data. The GDPR only applies to personal data and outright says that anonymized data is not considered personal data and therefore does not fall under the GDPR. Strictly speaking, capturing data is already considered processing and hence requires consent or another legal basis. We believe that anonymization at the source may in future be considered acceptable, if the anonymization can be shown to be effective. Consequently, we propose multiple technical measures that aid JCRS implementations in achieving anonymization.

One possible way of achieving anonymization can be reached if we intentionally worsen our radar resolution to such an extent to which it is improbable to detect or at least differentiate a person from other objects of similar size. However, it is important to note that if the radar sensing resolution is switchable between higher and lower quality the access to this configuration must be highly restrictive and secure. This is an obligation which shows that appropriate security measures must be taking to ensure that such a shift in sensing quality, and therefore a removal of anonymization, cannot be achieved without authority and consent of a high-level access to responsible controls.

Indirect Identification refers to situations where, despite efforts to anonymize data, there is still a possibility that individuals can be identified indirectly through the consideration of additional information or context. This is especially true in surveillance systems like JCAS in which the knowledge of someone being not at an expected location can already deliver too much sensitive personal data through sophisticated interference attacks. A simple example of this would arise if it is possible to check if a person is present in a specific area. This way if someone has additional information about the schedule of a natural person it can be checked if a person is in the location in which it is expected to be and from this interfere additional personal information. As can be seen, with indirect identification in mind improving data protection is often enhanced by removing data that can be linked with minimal effort to natural persons. Therefore, as second example, we are assuming that if there are two persons on a city square this information can much more easily be linked for example if we know that simultaneously there is a scheduled work time of two street cleaners. Contrarily, if there are 20 people in the square the additional information that we know about the street cleaners is much harder to directly link to them. Therefore, we suggest that for small groups of people in an area, only very rough estimates of the number of people present should be reported. Alternatively, or additionally, an inherent noise or stochastic randomness should be added to each reported number of people.

Another privacy measure for anonymization can be reached through the removal of tracking or tracing persons through JCAS. To achieve this, we want to propose two options. The first one is that we generalize objects of human size. So, any persons, bicycle, animal or car is treated as the same type of object. Secondly, it needs to be ensured that persons that enter or exit into private spaces cannot be linked to time and exact place or building. Implementation possibilities of this include fake information such as ghost images of people being shown going much further than is in fact true.

But only the blurring of the location tracking of natural persons itself is not enough. Further we need to consider the ability of analysing and collecting movement behaviour through JCAS systems. To prevent this sort of identifiability of natural persons, personal movement behaviour and quirks should be removed and deleted from the captured data through fitting filter. Such a filter would only forward location data and remove any observations on the individual itself. Especially a linking of such data into artificial intelligence models and algorithms is then not possible or made implausible.

Further Measures

If a complete anonymization is not possible or desirable, we need to consider the effort, exemplary time or cost, necessary to identify a natural person (for related juristic information see recital 26 of the GDPR). In this case any reasonable data protection and privacy measure which maximizes the effort necessary for a possible identification are of utmost importance. As such measures like including the addition of fake information or further limiting of information provided about individuals and their specific activities can increase the difficulty of identification. In the following we want to discuss various methods.

A weaker version of anonymization that has the same goal of hindering identification of individuals is pseudonymization. Fundamentally, pseudonymization allows for the data to retain identifying attributes, but requires these to be very hard to link back to the actual individuals. The main difference is that pseudonymization can be reverted by inversing applied functions and methods to the pseudonymized data. If pseudonymization is used, then the knowledge of reverting pseudonymized data can under no circumstances be leaked. For this case we recommend three basic data protection measures. First the pseudonymized data itself needs to be stored encrypted, with high access control. This also includes confidentiality and integrity of data in transit. Secondly the very same principle applies to the reversible functions and processes. Third, the pseudonymized data and the reversibility functions need to be stored in different places with different access mechanisms, to ensure resilience in case either one is leaked. This way if one is leaked the data can be reverted and pseudonymised again with different functions. To ensure the success of these measures, state-of-the-art security and intrusion monitoring systems should be installed. We consider pseudonymization instead of anonymization as a risk to privacy and therefore it should be used sparingly and carefully even with the mentioned measures in place. Strict regulations should exist for providers that plan to use JCAS data with pseudonymization.

Finally, we want to highlight that personal data should be acquired for specific and explicit purposes. Legally, this is also explained in article 5 b) of the GDPR. This can be implemented into JCAS services by only offering services for specific purposes. For example, if an autonomous vehicle needs sensing information from around a corner, it will not be interested in pedestrians walking on the sidewalk that make no attempt to cross the road. In the same sense it is not interested in the classification of the object that is on the street. The only knowledge it needs are the location and velocity of crossing objects. This way, less data is provided to subscribers of JCAS services. Linking and identification of natural persons is therefore hampered.

Conclusion and Summary

The presented use cases and their further examinations clearly show that JCAS, just as other sensor systems might be privacy invasive, if no countermeasures are taken. Note, that JCAS may also be able to offer existing services in a more privacy-friendly manner, than what is deployed right now. While a person's identification from a single snapshot alone might be more difficult, compared to a camera picture, the networked data from many JCAS systems could achieve this more easily. This finding leads to the conclusion that measures like anonymization have to be take to meet the presented regulatory restrictions. Though some examples of these measures are drafted in this paper, further research is needed to refine, implement and test these measures against the presented privacy threats.

Bibliography

[1] Y. C. Y. H. a. B. Z. Y. He, “WiFi vision: Sensing, recognition, and detection with commodity MIMO-OFDM WiFi,” *IEEE Internet of Things Journal,* vol. 7, no. 9, pp. 8296-8317, 2020.

[2] A. Hundepool, J. Domingo-Ferrer, L. Franconi, S. Giessing, E. S. Nordholt, K. Spicer and P.-P. de Wolf, Statistical Disclosure Control, John Wiley & Sons, Ltd , 2012.

[3] C. Dwork and A. Roth, The Algorithmic Foundations of Differential Privacy, Boston - Delft : Now Publishers Inc, 2014.

[4] M. Geiger, D. Schlotthauer and C. Waldschmidt, “Improved Throat Vibration Sensing with a Flexible 160-GHz Radar through Harmonic Generation,” in *2018 IEEE/MTT-S International Microwave Symposium - IMS*, Philadelphia, PA, USA, 2018.

[5] K. Han and S. Hong, “Vocal Signal Detection and Speaking-Human Localization With MIMO FMCW Radar,” *IEEE Transactions on Microwave Theory and Techniques,* pp. 4791-4802, 12 August 2021.

[6] C. Shi, T. Zhang, Z. Xu, S. Li, Y. Yuan, A. Petropulu, C. T. M. Wu and Y. Chen, “Speech privacy attack via vibrations from room objects leveraging a phased-MIMO radar,” in *Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services*, Portland, OR, USA, 2022.

[7] De Montjoye, Yves-Alexandre, César A. Hidalgo, Michel Verleysen, and Vincent D. Blondel. "Unique in the crowd: The privacy bounds of human mobility." Scientific reports 3, no. 1 (2013): 1-5.

[8] Ma, Yongsen, Gang Zhou, and Shuangquan Wang. “WiFi Sensing with Channel State Information: A Survey.” ACM Computing Surveys 52, no. 3 (May 31, 2020): 1–36.

[9] Zhang, Kuan, Jianbing Ni, Kan Yang, Xiaohui Liang, Ju Ren, and Xuemin Sherman Shen. "Security and privacy in smart city applications: Challenges and solutions." IEEE communications magazine 55, no. 1 (2017): 122-129.