Chapter 12
Privacy-Oriented Analysis of Ubiquitous Computing Systems: A 5-D Approach

Agusti Solanas, Edgar Batista, Fran Casino, Achilleas Papageorgiou, and Constantinos Patsakis

Abstract Ubiquitous computing systems are commonplace. They have opened the door to great benefits for society as a whole. However, they have to be used with care, otherwise they can cause serious risks for their users. In this chapter, we analyze the privacy risks of ubiquitous computing systems from a new individual-centred perspective based on five privacy dimensions, namely identity, location, footprint, query and intelligence. We describe each dimension and provide an introductory view of the main privacy risks of these systems. Also, we discuss some of the challenges that derive from new trends in the field.

12.1 Introduction

The widespread deployment of ubiquitous computing systems (UCS) is a commonplace reality. Despite their youth, the adoption of ICT together with the generalization of the Internet [294] have enabled the early consolidation of UCS in our daily lives. Nowadays, it is not surprising to find people using multiple computing devices: from traditional computers or laptops, to smart phones or even trendy smart watches or fitness trackers equipped with plenty of built-in sensors and powerful computing capabilities. In addition, to make things even more complex, interactions do not take place between humans and machines only, but among machines too. Those machine-to-machine interactions are magnified with the adoption of the Internet of Things (IoT), which implies a strengthening of the overall sensing capabilities of the machines ecosystem which allows further

A. Solanas
Universitat Rovira i Virgili, Tarragona, Catalonia, Spain

E. Batista
SIMPPLE, Tarragona, Catalonia, Spain

F. Casino · A. Papageorgiou · C. Patsakis (✉)
University of Piraeus, Piraeus, Greece
e-mail: kpatsak@unipi.gr

G. Avoine, J. Hernandez-Castro (eds.), *Security of Ubiquitous Computing Systems*,
https://doi.org/10.1007/978-3-030-10591-4_12

processing [437]. In a nutshell, the consolidation of these technologies has paved the way for what has been called the third era of modern computing [424].

Following the increasing use of UCS, it was inevitable that they would become able to sense, collect and store huge amounts of information, which quite frequently refer to people. From a global perspective, this results in a tremendous increase in the data generated (and stored) in the digital world and, in fact, according to IBM, by 2017 90% of all data ever created had been created just in the previous 2 years [290]. It is worth noting that most of this data is sensor-based data gathered by UCS. In this situation of rapid growth of heterogeneous data, big data technologies has emerged as a solution for their management and processing [293].

People, consciously or not, provide vast amounts of personal information (e.g., locations, preferences) to digital services in exchange for an improved user experience and personalized results. In the UCS context, the storage and processing of large amounts of data could jeopardize privacy. Thus, it must be preserved by computer systems and technologies should be revisited as they evolve to guarantee individuals' privacy and to foster awareness. Interestingly enough, about two decades ago, in the late 1990s, initial studies evaluated people's awareness regarding privacy in the digital world due to the rise of the Internet and e-commerce. This was done by profiling individuals [351] and evaluating their *comfortability* in providing different types of information [8]. At that time, people could have hardly imagined the effects of the new digital era and its influence on today's lives. Thus, recent studies aim at evaluating the levels of concern of people regarding ubiquitous tracking and recording technologies [438], and their main concerns regarding their loss of control over their privacy [352]. Currently, the adoption of big data motivates the redefinition and analysis of privacy concerns on UCS [400].

Already identified as one of the most challenging issues, privacy is not a new addition to the ubiquitous computing field [578]. Unfortunately, determining whether a given UCS is privacy-friendly is not straightforward, since current techniques are based on individual analyses. In this context, understanding the purpose of UCS, how they work, and why they work that way, are key questions that emerge from the analysis of their privacy features [348, 513]. The increasing number and variety of UCS makes the assessment of the proper management of personal data in all UCS devices very difficult. Additionally, new advances in the privacy and security fields (e.g., recent attacks, vulnerable technologies and protocols) do not guarantee to an adequate level that a certain UCS will always remain safe, and this motivates the periodical review of UCS privacy-related analyses. It should also be highlighted that the recent implementation of the General Data Protection Regulation [547] requires the privacy impact assessment of all services that process sensitive user data, along with other requirements such as consent management, mechanisms to allow data portability, and erasure of user data [486]. All in all, interest in UCS privacy is justifiably growing.

12.1.1 Goal and Plan of the Chapter

In this chapter we analyze the current state of UCS from a privacy perspective. To do so, we identify, describe and explain the most relevant privacy risks that derive from the deployment and use of UCS. However, since privacy is a multifaceted topic, understanding it holistically might be difficult for non-expert readers. Hence, we propose the use of a 5-dimensional approach to analyze privacy and we classify the identified privacy risks into five privacy dimensions: *identity privacy*, *query privacy*, *location privacy*, *footprint privacy*, and *intelligence privacy*. This 5-D approach, which has been previously used in the context of smart cities, will help readers grasp the difficulties and nuances of privacy protection in a compartmental way, which will finally lead to a wider and more comprehensive understanding of the problem. Therefore, the ultimate goal of the chapter is to increase awareness on privacy risks related to UCS.

The rest of the chapter is organized as follows: Sect. 12.2 summarizes previous work related to the identification of threats in UCS and reports the most relevant classifications and analysis of privacy-related issues. Section 12.3 describes our 5-D classification of privacy risks in UCS. Moreover, possible countermeasures, some practical scenarios and privacy enhancing technologies will be discussed, to better illustrate each privacy threat. Next, Sect. 12.4 provides readers with a glimpse into the future of privacy protection in the context of UCS, by analyzing the impact of new technologies and services. Finally, the chapter ends in Sect. 12.5 with a summary of the main contributions and with some thoughts regarding the importance of increasing awareness on privacy-related issues in UCS.

12.2 Background and Previous Work on Privacy in UCS

Regardless of the context or application area of the UCS at hand, its design involves several challenging steps, from the proper selection of hardware and technology (e.g., microelectronics, power supplies, sensors, communications, localization technology, M2M interactions and human-machine interfaces [518]), to the implementation of a system that addresses security risks [119, 352] (e.g., large number of nodes, resource constraints, authentication-related challenges, unauthorized access to devices or networks) and privacy issues. Regarding the latter, some studies have analyzed the privacy issues of UCS. Kušen and Strembeck published, very recently (i.e., 2017), a systematic literature review on the security of UCS and they identified vulnerabilities, threats, attacks, and some defenses. Within the last category they consider several options (i.e., trust computation and management, cryptographic protocols, authentication and access control, and privacy protection mechanisms).

They identified the most common privacy protection mechanisms found in the literature [352] as follows:

- Masking mechanisms that preserve individuals' privacy by hiding their identities.
- Privacy protection layer for mobile apps, that imply security analyses, configuration and proper regulation of permissions. Especially when it has been repeatedly proven that leaks are common [459].
- Obfuscation, based on deliberately degrading the quality of the information.
- Proximity detection schemes, that are founded on trust computation based on *encounters*, which require a coincidence in space and time and a mutual interest between the components performing the computation.
- Game-based approaches, to find the optimal privacy protection mechanism depending on the requirements and needs of participants by following several rounds in a game between the attacker and the user.
- Consents and notifications.
- Negotiation approaches, in which privacy settings may be modified and configured to enable different services.
- RFID-based methods, that use RFID devices that simulate multiple RFID tags simultaneously.
- Other techniques such as tag identification schemes or recommendation systems for private location-sharing services.

In this study, the authors found that 29% of the privacy measures were related to masking mechanisms, these being the most frequently used. Although most research on privacy in UCS is focused on the aforementioned privacy protection mechanisms, it is worth noting that privacy may also be considered as a requirement by design. Along this line, Duan and Canny[190] advocate for the principle of *data discretion* in which, in their own words, *"users should have access and control of data about them, and should be able to determine how it is used."*.

Moreover, in [357] Langheinrich stresses the importance of including privacy considerations in the early stages of system design. He proposes six principles to guide the development of privacy-preserving ubiquitous systems as follows:

- Notice: Users should always be aware of what data is being collected.
- Choice and Consent: Users should be able to choose whether it is used.
- Anonymity, Pseudonymity: Should apply when identity is not needed.
- Meeting Expectations: Systems should mimic real-world norms.
- Security: Different amounts of protection depending on the situation.
- Access and Recourse: Users should have access to data about them.

Also, Langheinrich, in [358], proposed a privacy awareness system (PawS) to enforce users' participation and to give them the ability to respect other user's safety, property, or privacy, and to rely on social norms, legal deterrence, and law enforcement to create a reasonable expectation that people will follow such rules.

In addition, PawS elaborates on four principles that complement the previous and that are prevalent in a ubiquitous computing environment:

- Notice: The ability of the environment not only to set privacy policies but also to implement efficient ways to communicate these to the user.
- Choice and consent: The provision to the data subject of the choice and ability to agree or to oppose a policy in a functional way.
- Proximity and locality: Mechanisms to encode and use locality information for collected data in order to achieve access restrictions based on the location of the person.
- Access and recourse: The system must give access to the user's data and also provide him with all of the essential information regarding the activity history of the usage of his data.

For the above principles to be fulfilled Langheinrich suggests a series of mechanisms, namely machine-readable privacy policies, policy announcement mechanisms, privacy proxies, policy-based data access.

In UCS we want technologies to fade into the background and become invisible to the user, hence, the location of the user should not be an obstacle. In this sense, Location Based Services (LBS) [346] are one of the main enablers of UCS. The research on privacy protection in LBS is vast [29, 342, 460, 533, 573]. In this line, several dimensions of privacy could be identified [395, 461] but in most cases, research articles focus on only one at a time: identity [76, 85], data [454, 484, 571], location [30, 408, 506, 599] and footprint [7, 123].

12.3 5-D Classification and Analysis of Privacy Risks

From Sect. 12.2 it can be derived that most of the efforts have been oriented towards the suggestion of measures to protect privacy (fighting against specific privacy issues). Also, some efforts have been devoted to the analysis and proposal of privacy principles and properties to be fulfilled. However, there is a lack of conceptual models that allow researchers and practitioners to analyze UCS privacy holistically. With the aim to fill this gap we build upon the ideas of Martínez et al. in [395] to suggest a 5-dimensional privacy model for UCS.

The 5-dimensional privacy model results from the combination of two simpler privacy models (i.e., the 3-D Conceptual Framework for Database Privacy [187] and the W^3-privacy model for location-based services [461]), and it was already used within the context of smart cities [395]. However, in this chapter we revisit the model and adapt it to the nuances of UCS. Moreover, we provide more detailed insights regarding the scope of each dimension with regard to individuals' privacy, in opposition to corporations' privacy, which in the original model was called "owner privacy" and we have renamed it for the sake of clarity as "intelligence privacy". In our model, we identify five privacy dimensions: (1) *identity* privacy, (2) *query* privacy, (3) *location* privacy, (4) *footprint* privacy, and (5) *intelligence* privacy. Next, for each dimension, we detail the definition, risks, countermeasures and practical scenarios within the context of UCS.

12.3.1 Identity Privacy

In the context of UCS, service providers cover some needs of their clients through a variety of added-value services. In order to use such services, generally, providers require clients to identify themselves using different kinds of identification mechanism to control who is accessing the services. Although this requirement is reasonable in most cases from the providers' perspective, it might not be always convenient from the users' perspective, they might prefer to avoid the disclosure of their identities.

Identity privacy refers to the preservation and non-disclosure of the identities of individuals to service providers when using their UCS-based services. The identification of users (e.g., by using their full name, the SSN) commonly improves their experience since it enables the outcomes of the service to be personalized in accordance with users' preferences. However, identification procedures based on this kind of personal data allow providers to uniquely identify their clients and track their use of the provided service (or services). As a result, privacy advocates have raised concern about user profiling.

Disclosing real identities to service providers enables the possibility for those providers to create digital profiles with personal information and, as a result of combining information from multiple providers (or from multiple services offered by the same provider) they could infer personal information such as daily activities, habits and routines. The more information providers collect and the more UCS services deployed, the more accurate and realistic these digital profiles can become. With the creation of users' profiles, additional concerns such as the trustworthiness of the providers, the purposes of the gathered data, and the potential privacy impact in the case of misuse or theft arise.

Using pseudonyms might help to preserve identity privacy. However, this is a choice that is frequently not in the hands of users but providers, who decide which information they require for validation. The idea behind pseudonyms is simple and builds upon linking a certain pseudonym or pseudonyms to an individual's identity in a secret, unique and non-trivial way. Users might create and control their own pseudonyms, but this task might be difficult for most users and it is handed over to pseudonymisers (i.e., third parties that do the job). In this case, the trust is placed in those pseudonymisers. Hence, using a single pseudonymiser might not be enough for some users. With the aim to improve the privacy-resistance of a single-pseudonymiser approach, multiple and geographically distributed pseudonymisers can be used instead [462].

It is worth noting that often users are identified by means of the devices they use. We observe several risk levels depending on the nature of the UCS device in place. The riskier situation arises with UCS devices that normally belong to a unique individual (e.g., smart watches, smart glasses or fitness trackers). In this situation, to preserve the identity privacy of individuals, the relationship between each individual and his/her device must be unknown. Hence, pseudonyms could be helpful but clearly are not enough to prevent the disclosure of identities. A similar, though not so risky scenario is that where we have UCS devices providing services to a controlled group of people, such as the UCS devices in a smart home or in an autonomous vehicle. In this scenario, services are provided to their owners. As in the previous situation, the relationship between individuals and devices should be unknown. However, in this case, if the service identifies the device, it cannot identify a single individual, since he/she is somehow anonymized within the group. The more people using the same device, the more preserved their identities will be. This example could be extended to larger systems such as smart cities in which services are provide to the entire population in which case, the identity of the users is practically guaranteed. Despite the above, we suggest the use of attribute based credentials [84, 244] as the best option to protect identity privacy in the UCS context, especially when using a single device.

12.3.2 Query Privacy

Usually, UCS provide services on demand, i.e., upon the reception of requests from consumers. Normally, these requests can be understood as queries that users create to obtain a specific service. Although queries do not necessarily include personal identifiers, they have to be managed carefully since they could disclose much personal information. In this context, *query privacy* refers to the privacy preservation of the queries sent by users to UCS service providers.

By collecting queries from anonymous users, one could profile them and infer their habits and preferences. More importantly, some queries could enable the identification of such "anonymous" users [9]. In this situation, users tend to trust providers, however, this has proven to be a suboptimal solution. Thus, with the aim to avoid the need to trust providers, scenarios where services can be used by providing minimal query information would be suitable from the privacy perspective (i.e., putting in place the principle of data minimization). By doing so, users make more difficult for service providers to learn information.

Most users are not trained to tune their queries, hence, in general, *query privacy* concerns can be mitigated by using Private Information Retrieval (PIR) techniques. By definition, PIR-based schemes are cryptographic protocols that retrieve records from databases while masking the identity of the retrieved records from the database owners [589]. From the UCS-based services perspective, PIR tools could be used by consumers to query service providers. By doing so, the correlation between queries and individuals could be broken and profiling becomes much more difficult.

Queries and their results can be easily analyzed by UCS-based service providers unless the proper countermeasures are put in place. For example, providers of fitness services could infer habits and routines when interacting with the fitness trackers since they collect a variety of health-related data (e.g., physiologic, biometric, exercise, calorie intake). Furthermore, UCS-based services in smart homes and autonomous vehicles might also put in danger *query privacy* since the submitted queries could be used to extract information about daily habits, such as work schedules or sleep routines. Finally, one of the most challenging UCS services that could endanger *query privacy* are those related to voice recognition, since they listen to and record the exact query. For this kind of service, it would be necessary to guarantee that the signal processing is done on the device, which currently is not the case for most services.

12.3.3 Location Privacy

One of the most significant revolutions provided by UCS is their capability to bring computation anywhere. The deployment of UCS devices around the globe has indirectly led to the control and monitoring of their physical location.

This situation may raise some privacy concerns since location of users of such devices could be inferred. Location data needs to be carefully managed. It is worth noting that with location information, other sensitive data could be inferred, e.g., health-related data, religious or political beliefs, or even social relationships. The importance of preserving individuals' location privacy in the context of UCS-based services justifies its addition as an independent dimension to be analyzed. *Location privacy* concentrates on guaranteeing the preservation of the physical location of individuals when accessing UCS-based services.

Classical location-based services (LBS), which could be integrated into UCS devices, require location data to provide their services (e.g., roadside assistance, real-time traffic information or proximity-based marketing). Normally, UCS service providers receive location information directly from individuals that use their services. For instance, requiring the weather forecast information or the best route to go to a specific location according to the real-time state of the traffic are services where individuals disclose their location information explicitly. Besides, many UCS devices, such as smartphones, smart watches, fitness trackers or autonomous vehicles, already integrate built-in sensors with location capabilities, commonly GPS-based.

Moreover, there are situations in which UCS providers could infer the location of individuals by using proximity data. For instance, video surveillance systems could identify individuals (e.g., by using face recognition) and associate their location with that of the camera, without the intervention of the user. Also, in the case of autonomous cars and smart homes, the location of users is indirectly disclosed since it coincides with the location of the car and the home, respectively.

The sensitiveness of location data fosters the search for solutions that allow the hiding of location information while preserving functionality. For example, in scenarios where the location of the UCS changes over time, collaboration mechanisms between nearby UCS devices/users could mask exact locations, so that the location data sent to the providers would not directly disclose the real location. Similarly, if collaboration protocols are not suitable, real locations could be also protected by means of cloaking services [248] or by determining the proximity to entities without revealing their whereabouts [342, 460]. However, this could result in a degradation of the quality of the results obtained and users might look for the right balance between location details disclosure and the quality of the results.

12.3.4 Footprint Privacy

While providing clients with the requested services, service providers collect information about them. They store the activities that individuals perform, mainly for traceability and analytical purposes. As a result, large amounts of microdata (i.e., individual records containing information collected from individuals) are stored. Roughly speaking, UCS providers collect microdata sets with information detailing the use and traffic on their services, that is, the footprint left by the users on the services. Privacy concerns might emerge once these microdata sets are published or released to external third parties, since these parties could be able to retrieve meaningful information about individuals. In addition, if third parties obtain microdata sets from several service providers used by the same user, further knowledge could be inferred about the individuals' actions. To address these concerns, *footprint privacy*, considers the control of the information that can be retrieved or inferred from microdata sets.

Any UCS service provider collecting and storing information about the activities of their consumers might raise footprint privacy concerns. In previously discussed privacy dimensions, users played a key role in protecting their privacy by putting in place the right countermeasures. However, in the footprint privacy dimension, most of the effort to guarantee privacy is handed over to the provider, and hence it has to be enforced by law (as in fact it is). This privacy dimension will mainly be preserved when service providers apply the proper countermeasures before releasing microdata sets. Otherwise, the privacy of individuals whose data have been collected would be jeopardized.

Statistical disclosure control (SDC) techniques have been used to protect the privacy of users, whose data is stored in microdata sets. Footprint privacy is, hence, normally preserved by applying those techniques. Proposed SDC techniques (e.g., noise addition, rank swapping or micro-aggregation [534], to name a few) aim to prevent linkage between individuals' identities and some of their data (i.e., footprint data) by distorting it. It is worth noting that footprint data does not include identifiers. However, the combination of quasi-identifier attributes might lead to the reidentification of users. Yet, the distortion applied to the data to enhance privacy is not free, since the quality and the utility of the data decrease. So, when using SDC techniques a trade-off between privacy and data utility needs to be considered [287].

12.3.5 Intelligence Privacy

In the current globalization context, there are numerous service providers offering similar products and services, which results in an increase in the number of competitors. Data collected by each provider is, in many cases, very valuable, and it is used to extract knowledge and provide customer-oriented, personalized or added-value services. Hence, sharing and releasing this data is not a common practice, especially if competitors have a chance to take advantage from such data. However, in some cases, organizations (not necessarily competitors) could take mutual benefit by collaborating, but they do not want to share their data. This situation is covered by what we have called *intelligence privacy*. In this dimension, the goal is to allow the collaboration among several organizations so that all could make joint queries to databases to obtain joint information in such a way that only the results are revealed (i.e., the actual information in the databases of each company is not shared or revealed).

To clarify the concept of intelligence privacy let us have a look at the following example of manufacturers of autonomous and intelligent vehicles. Each vehicle manufacturer integrates many built-in sensors on vehicles to gather, store and analyze the status of the car, the nearby environment and further driving-related parameters. Since these data are highly sensitive, manufacturers might decide not to share them. However, collaboration among manufacturers by sharing data could be extremely useful to improve safety on roads and to avoid collisions. In this sense, each manufacturer (even if they compete) would benefit from the collaboration, that is, to obtain joint results, but they want to avoid sharing their intelligence data.

In this situation of mutual distrust, Privacy-Preserving Data Mining (PPDM) techniques emerge as the natural solution to protect *intelligence privacy* [12]. PPDM methods are applicable once independent entities want to collaborate to obtain common results that benefit both of them, but without sharing their data since they do not trust each other. In such scenario, by applying PPDM to the queries submitted across several organization databases, the amount of information transferred to every party is controlled, and this does not pose risks that original data will be revealed, only the results.

It is worth emphasizing that *Intelligence Privacy* considers data belonging to companies (e.g., the heat dissipated by the front-left wheel brake). Thus, data collected by companies but belonging to individuals should not be considered under this dimension because they belong to the users and not to the companies, and hence they should be managed as such.

12.4 Future Trends and Challenges

Privacy has often been considered from a data-oriented perspective. The goal was to protect the data regardless of their origin. Data, in this sense, were seen as something of value that belong to whoever has the ability to collect, store and exploit them and, following this line, privacy protection has been mixed with related problems such as access control, network and database security, and the like. However, to understand privacy we have to put the focus on people and, from there, we should rethink the whole architecture that aims at protecting it.

Although some people support the idea of companies' privacy (i.e., our concept of *intelligence privacy*), privacy issues mainly affect people. There is no doubt about the importance of protecting people's privacy and to do so we state that the focus should be put on people and become personalized. In the years to come, we will see many changes related to how privacy is understood, how the focus will shift from data privacy to people's privacy, and how the latter is protected in practice. We see some fundamental changes that are taking place already and are going to fully develop in the years to come.

12.4.1 Privacy by Design

The addition of privacy at the very beginning of the design process [357] is going to change many ideas and bad practices that are common nowadays. This principle is especially important when we consider the UCS that surround us all the time. Take as an example the face recognition technology that allows access to our mobile phones. In the early days of this technology (and similar ones), biometric information was sent to servers over the Internet, analyzed, and the authentication result was sent back to the edge device. Clearly, this procedure has many points of failure from a privacy perspective. Now most of these technologies are executed on the device, and as a result the data is privately stored by the user and privacy risks are lessened. Emerging technologies based on context-awareness (e.g., smart homes, smart cities, intelligent transportation systems, smart healthcare systems [535, 536]) must be designed with privacy at their core, otherwise we will make the same mistakes of the past and we will need to address privacy as an additional layer outside the system instead of an inner component.

12.4.2 Individual-Centred Privacy

We are shifting towards an individual-centred privacy in which the focus is on the user of the technology and privacy is going to be protected by understanding the personal dimensions of users. As we introduced in this chapter, those dimensions respond to questions such as Who am I? (Identity Privacy), Where am I? (Location Privacy), What do I need? (Query Privacy), What have I done? (Footprint Privacy). This paradigm shift is especially relevant when we consider the impact of wearable devices (e.g., smart phones, smart watches, smart glasses). Most of the data that they generate are sensitive, personal data about their users, hence the important thing here is not the data per se but its relationship to users and their privacy dimensions.

12.4.3 Growing Importance of Legislation

Since the beginning of the twenty-first century, researchers have proposed concepts such as data minimization to improve privacy protection. However, these ideas are taking shape along with others such as consent as a result of the enforcement of the Global Data Protection Regulation (GDPR) [547]. In this sense, it could be said that the ideas were there, but it took almost 20 years to provide them with the right embodiment to be enforced. Clearly, the role of legislation and law enforcers will be fundamental for the protection of privacy, since technology alone can hardly protect all privacy dimensions that affect people.

Lately, there has been a lot of controversy around the impact of the GDPR in the technological context, affecting trendy fields such as UCS, IoT and Big Data. With the aim to enhance individuals' privacy and strengthen the protection of personal data, GDPR unifies data protection laws across EU member states. Law experts agree that GDPR has caused a major overhaul of data protection laws across EU. Thus, to preserve individuals' privacy and guarantee their rights, UCS need to be designed to protect individuals data.

To prevent potential data misuse, GDPR limits the processing of personal data, places higher importance on individuals' consents, and strengthens the rights of individuals to control their data. Also, it introduces reinforcements on the conditions for processing personal data. Hence, processing is only allowed when individuals give explicit and informed consent for such processing according to some well-defined and unambiguous purposes and uses. These requirements pose many challenges for UCS (e.g., obtaining consent in public environments, clearly defining the purposes of processing). In addition, GDPR introduces the right to withdraw this consent (i.e., revocation of consent) easily and at any time, thus denying the future processing of these data if no legal basis justifies their storage.

Also, GDPR considers the right of individuals to obtain their data in a structured, commonly used, interoperable and machine-readable format. This is indeed very challenging, since the heterogeneity of UCS leads to a wide spectrum of information to be returned, ranging from health-related data, wearable trackers, and opinions to even biometric and financial data [562].

For the processing of personal data, UCS must put in place appropriate means to guarantee privacy. For instance, encryption and pseudonymisation could be used to ensure confidentiality. However, despite these techniques, UCS are not free of attacks that open the door to personal data breaches and scenarios where data is compromised. In this context, considering that GDPR establishes the obligation to communicate data breaches to supervisory authorities within 72 h, monitoring systems should permanently keep track of UCS activities and look for abnormal behavior that could compromise personal data [176].

The effect of GDPR on privacy protection will be varied, and the years to come will see a very interesting transformation of the field of privacy protection as a result of its deployment and enforcement.

12.5 Conclusions

Privacy is a fundamental right that has to be protected, and Ubiquitous Computing Systems (UCS) are so intricately fused with our daily lives that they must play a key role in this endeavor. In this chapter, we have provided an overview of the privacy issues that might arise as a result of the generalization of UCS.

We have briefly summarized the state of the art on the matter and we have proposed a 5-dimensional framework that allows the analysis of privacy protection from an individual perspective, in opposition to the older approach centred on data. In our model, we focused on individual dimensions (i.e., identity, location, query, and footprint). Also, for the sake of completeness we have considered a dimension for companies (i.e., intelligence privacy). We believe that this high-level model of privacy dimensions will help researchers and practitioners to approach the difficult problem of analyzing and guaranteeing individuals' privacy in a more comprehensive way.

Also, we have analyzed some of the main changes that we expect to affect privacy in UCS now and in the years to come. Along this line, we emphasized three fundamental trends, namely the consolidation of the privacy-by-design approach, the paradigm shift from data privacy to individuals' privacy, and the growing importance of legislation. Overall, this chapter had the goal of improving people's awareness on privacy issues that affect us all. We hope that these lines have helped readers realize the importance and fragility of their privacy in the technological world in which we live today.