ARTICLE IN PRESS

Pervasive and Mobile Computing ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

journal homepage: www.elsevier.com/locate/pmc

Privacy protection in pervasive systems: State of the art and technical challenges

Claudio Bettini, Daniele Riboni *

Università degli Studi di Milano, D.I., via Comelico 39, I-20135 Milano, Italy

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Data privacy
Anonymity
Obfuscation
Pervasive applications

ABSTRACT

Pervasive and mobile computing applications are dramatically increasing the amount of personal data released to service providers as well as to third parties. Data includes geographical and indoor positions of individuals, their movement patterns as well as sensor-acquired data that may reveal individuals' physical conditions, habits, and, in general, information that may lead to undesired consequences like unsolicited advertisement or more serious ones like discrimination and stalking.

In this survey paper, at first we consider representative classes of pervasive applications, and identify the requirements they impose in terms of privacy and trade-off with service quality. Then, we review the most prominent privacy preservation approaches, we discuss and summarize them in terms of the requirements.

Finally, we take a more holistic view of the privacy problem by discussing other aspects that turn out to be crucial for the widespread adoption of privacy enhancing technologies. We discuss technical challenges like the need for tools augmenting the awareness of individuals and to capture their privacy preferences, as well as legal and economic challenges. Indeed, on one side privacy solutions must comply to ethical and legal requirements, and not prevent profitable business models, while on the other side it is unlikely that privacy preserving solutions will become practical and effective without new regulations.

1. Introduction

In our everyday life, independently from our attitude towards technology, we inevitably release personal information either by filling in a job application, by obtaining a shop fidelity card, by passing through a toll-road, by using a credit card or just by walking in shopping malls and public streets where tens of cameras are deployed. In principle, this information may be improperly used in a number of ways including unsolicited advertisement, discrimination, identity theft, or even stalking. This is not a new situation, but the advance in technology has dramatically increased not only the amount of personal information that is acquired, but in particular the ability to store, process, and share this information. Cloud computing and social networks in particular have given a boost in the collection, sharing and processing of personal information that inevitably lead to several privacy breach accidents. For this reason, privacy, generally defined as *the right to be let alone*, is becoming more and more a shared concern. Nonetheless, a recent review on mobile apps for healthcare and well-being has shown that a relevant part of both free and paid apps does not expose any privacy policy; many of them send data to undisclosed third parties; and the vast majority of them transmits potentially sensitive data in plain text [1].

A natural question for our readers is what is the role of mobile and pervasive computing in this situation? Indeed, independently from the success of cloud computing, social networking, and the big data analysis that they enable, we are

* Corresponding author. Tel.: +39 0250316350.
E-mail addresses: claudio.bettini@unimi.it (C. Bettini), daniele.riboni@unimi.it, riboni.daniele@gmail.com (D. Riboni).

http://dx.doi.org/10.1016/j.pmcj.2014.09.010
1574-1192/

witnessing a shift of paradigm in computer science. In 2011, smartphones and tablets outsold workstations and portable computers by 1.5×. In 2013, this ratio reached 4×. A major share of the smartphone apps has rich functionalities exploiting location, time, and other context parameters. An increasing number of objects, from consumer electronics to home appliances, from clothes to accessories are acquiring sensing, computing and communication capabilities; Wearable sensors monitoring fitness activities, sleep disorders, motion patterns as well as user's physical parameters are becoming trendy. We start seeing our home and office infrastructure sensing and communicating energy consumption patterns, presence patterns and in general information about what its inhabitants are doing. Analogously, the city we live in is using more and more sensing technology to become aware of what its inhabitants are doing with the noble goal of optimizing its services and improve safety.

It is quite intuitive that this shift of paradigm is indeed having a deep impact on how we share personal data and on how we will be sharing it in a few years. This impact has been perceived not only by technology experts, but by sociologists, economists and last but not least by law regulators. A growing number of people are concerned about the negative consequences that may arise from the large-scale monitoring of individuals' life in terms of human rights and societal values [2]. The 2014 White House report on "Big Data and Privacy"[1] also highlights the challenges for data protection that the collection of personal data through pervasive technologies implies. A major data protection reform has been recently proposed for adoption in the EU,[2] and analogous initiatives are being discussed all over the world. It is indeed a major question if technological solutions alone can address the privacy problem; it is our responsibility as researchers in this area to identify and explain the possible privacy threats that may be hidden in pervasive applications. Not only this could help in designing a modern regulation system that protects users without preventing new business opportunities, but it would also help software developers to design applications that better inform the user about possibly hidden consequences in terms of personal data release, and possibly mitigate the risk of privacy violation. This paper is intended to give a contribution along these lines.

The rest of the paper is structured as follows. In Section 2 we identify different categories of pervasive and mobile applications, the privacy threats that they may pose, and the requisites that should be considered when designing a privacy protection strategy. Section 3 critically analyses the state of the art for the privacy enhancing technologies applicable to pervasive applications with a specific reference to the identified requirements. The gap between the state of the art and the actual requirements is discussed in Section 4 describing open issues and research challenges, including economic, legal, and usability aspects. Section 5 concludes the paper.

2. Applications, privacy threats, and requirements

2.1. Identifying privacy threats

In this survey we consider a privacy violation to occur when the association between an individual's identity and some personal information is acquired, retained and/or processed by a third party without the consent by the individual. We refer to the third party as *the adversary*.

Despite new pervasive and mobile applications being proposed everyday as the result of the rapid evolution of sensing and mobile technologies, in this section we will make an effort to identify what we consider main application categories, and then analyze them in terms of the risks for privacy violation that they may involve. Understanding the possible presence of privacy threats includes understanding which parts of the information being released are considered sensitive to the user and which parts may be used to identify or re-identify (when joined with other information) the user. Since the actual presence of a privacy threat depends also on the entities that gain access to personal information, we will also mention the *possible adversaries* to be considered for each category. Indeed, no privacy protection technique can be properly validated if a clear adversary model is not provided. The model must specify at least: (a) which part of the personal information being transferred and/or processed the adversary has access to (e.g., complete/partial, occasional/historical, etc.), (b) which external or background knowledge the adversary has access to, (c) if different adversaries can collude.

Table 1recaps the main application categories, sensitive data, and adversaries, which are discussed below. Intruders, as well as third parties that may legally access the data, are considered adversaries for all categories of applications; hence, they are omitted from the table. Note that what was listed as sensitive data, may not be sensitive by itself, but may lead to a privacy violation when joined with external information. Moreover, sensitive data can lead to a privacy violation only when the adversary can link it to an identity. The table does not specify another kind of data released by these apps and that is referred in the literature as *quasi-identifier*. This is data that may be used by an adversary to re-identify the user (e.g., location itself may be used to restrict the candidate individuals being at that location in a given time instant). These aspects will be discussed in Section 3.

2.2. Location based services (LBS), mobile advertisement (MA), and Geo-social network applications (GeoSNs)

Characteristics: This is currently the category that includes most of mobile (and pervasive) applications since users and businesses have greatly appreciated the personalization of services based on user location. Examples of these apps are

[1] http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf.
[2] http://ec.europa.eu/justice/data-protection/.

Please cite this article in press as: C. Bettini, D. Riboni, Privacy protection in pervasive systems: State of the art and technical challenges, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.09.010

Table 1
Main application categories, sensitive data, and adversaries. Third parties and intruders are adversaries common to all categories, and are omitted from the table.

Acronym	Category name	Adversaries	Sensitive data
LBS	Location based services	Service provider	Location, absence, co-location
MA	Mobile advertisement	Service provider, merchant	
GeoSNs	Geo-social network applications	Service provider, other users	
PS	Participatory sensing	Data collector, service users	Location, sensed data
HC–WB	Health-care well-being	Service provider	Location, body-worn sensor data, activity
VA–SC	Vehicular applications and smart city services	Other drivers, city and road authorities	Movement traces, driving behavior, user habits
SH–SG	Smart home and smart grid applications	Power companies, home automation service providers	Occupancy, habits and activities

location and context-aware tourist apps, navigation apps, proximity based recommendation and advertisement apps. More and more users are also appreciating the ability to share location data in terms of check-in based mechanisms (like Foursquare or Facebook Places) or even through continuous location reporting (e.g., fleet management, friend-finders, co-operative navigation). From a pervasive system perspective we should keep in mind that location and time are only two of the parameters that compose the context of a user interaction with a service and that most considerations extend to other parameters.

Privacy threats and adversaries: The association of a user with a specific location at a given time can reveal health problems, affiliations, habits, etc. The availability of locations in real time as well as the historical data about user movements even introduces threats such as assault. GeoSNs exacerbate the risks, as the spread of location information occurs more easily and is less controllable. The term *location privacy* denotes the sensitivity of the association between a user's identity and the user's location, be it the user's past, current, or anticipated future locations. Knowing the location of a user also has implications for where the user cannot be located (*absence privacy*). This introduces the risk of burglary of unattended locations such as homes. Location information can also be used to determine sensitive associations among users. Thus, user location traces may reveal that certain users have been together, possibly frequently and for extended time periods. The term *co-location privacy* refers to the privacy of co-location events. In general LBS, the service provider is the only entity receiving the location data, and hence it is the typical adversary together with third parties that may legally or illegally obtain the data from it. In Mobile Advertisement the merchant may be an additional adversary; while it has to know how many users received an Ad, it should not necessarily know the user identities and their movements. In GeoSNs, georeferenced personal data may be exposed to many users; hence they should be considered adversaries as well. Surveys on privacy preservation for these applications are provided in a recent book [3] and by Wernke et al. [4].

Requirements: LBS typically have precision thresholds that strongly depend on the service. e.g., an online navigation service requires exact real time position while a localized news service works well with approximate location. Several LBS require either user identity or a pseudonym in order to personalize the service based on profiles. MA requires reporting to the merchant the number of different users receiving each Ad as well as the number of views. Different GeoSN services may have different requirements, in terms of location and time precision tolerance, as well as for the user identification.

2.3. Participatory sensing applications (PS)

Characteristics: Participatory sensing is becoming a paradigm for performing distributed sensing and it usually relies on a large number of individuals to provide data collected by their mobile sensor-equipped devices, and on a data collector entity to receive and process the global set of data. The same entity usually offers a service based on the resulting dataset. For instance, a thematic map of noise levels in different areas may be constructed from data obtained from users' smartphones or smart watches; similarly, air quality, temperature, or traffic conditions may be obtained for large areas. With a sufficiently large set of participants and widespread adoption of sensor equipped devices, participatory sensing enables very powerful applications both for real-time monitoring and for data analysis.

Privacy threats and adversaries: The willingness of a user to participate is not only dependent on the resources he has to provide (in terms of computing and communication costs) and on the offered incentives, but it is also related to privacy concerns. Due to the inherent mobile feature of the platform, sensed data need to include position and time of the device and these are usually the same as for its user, leading to location privacy threats. The sensed data may also contain contextual information that may be used to further refine location information (e.g., indoor/outdoor based on temperature) or may be sensitive by itself if associated with the individual (e.g., by revealing its emotional/physical condition). Possible adversaries are the data collector, the users of services based on the collected data, and, of course, any third party that legally or illegally gets access to the data collector databases. A good survey of privacy in participatory sensing is provided by Christin et al. [5].

Requirements: These applications need a mechanism to provide incentives/rewards to the user and to account for reputation as a data source. This somehow limits solutions based on pure anonymity.

Please cite this article in press as: C. Bettini, D. Riboni, Privacy protection in pervasive systems: State of the art and technical challenges, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.09.010

2.4. Health-care and well-being pervasive applications (HC–WB)

Characteristics: This class of applications usually involves data collected using body-worn sensors and smartphones possibly complemented with environmental sensor data. In some cases cameras and audio are also used. Several health-care projects have focused on supporting 'aging in place' as well as monitoring patients in non-critical conditions in their homes. Well being applications include monitoring fitness and activity related parameters. Applications may simply collect data to be processed server-side or may perform pre- or even complete real-time processing on the user device. Processing includes, for example, the recognition of the activity that the user is performing, abnormal conditions that require issuing alerts (e.g., falls or repeated signs of inability to properly carry out normal tasks), or, in the case of well being, estimating the consumed calories. A comparative review of smartphone apps for health and fitness is provided by Kranz et al. [6].

Privacy threats and adversaries: For health care applications the medical team or more generally the caregivers are usually considered trusted and the patient ID is known to them. The main threat is to release information regarding the individual's condition to non-authorized entities or to release sensitive information not strictly needed for the specific application. This is usually what happens when invasive technologies like video and audio are employed. Further sensitive health information may be inferred based on long-term patterns derived from body-worn sensor data. For instance, sleeping patterns inferred by wearable sleep monitors may reveal disorders like insomnia, stress, and compulsive obsessive disorders [7]. For well-being applications the service provider may also be considered an adversary in addition to the general public. The main threat is usually to release information on an individual's physical condition that may lead to discrimination if obtained, for example, by insurance companies. Many fitness applications also collect the geographical movements of the users. These impose similar threats as the LBS discussed above.

Requirements: HC applications in most cases require user identity to be revealed to the caregivers while WB applications may still hide the identity, using pseudonyms for profiling. Access control, anonymity and other data protection techniques, analogously to general medical data, should be used when storing and distributing information when necessary. HC applications are usually targeted to elderly people, and another main requirement is the simplicity of the interaction between the user and the devices/sensors. Limiting invasiveness of monitoring and sensing is often also a necessary condition for acceptance of the technology.

2.5. Vehicular applications and smart city services (VA–SC)

Characteristics: Vehicular applications currently belong to two main categories: traffic safety and traffic optimization. In both cases most models are based on VANET in which messages are exchanged between vehicles in addition of being possibly received also by road infrastructure. Since modern vehicles are equipped with hundreds of sensors, a huge amount of data is collected real-time in addition to the position of the vehicle itself. Traffic optimization and available parking search are also examples of smart city applications and they can be enabled by collecting data from vehicles.

Privacy threats and adversaries: Despite security being probably the main issue for these apps (e.g., avoiding intruders to send fake messages and generate accidents), there are privacy issues involved as well. Vehicles are in a sense similar to smartphones, since their position in many cases reveals the position of their owner. Other sensed data coming from these sources can convey information about the owner (e.g., even minor traffic violations). The adversaries are the other users, since their vehicle may actually directly receive the messages and they may also collude. In some cases also the road/city authorities may be perceived as an adversary for what concerns privacy issues. A survey by Domingo-Ferrer and Wu [8] illustrates safety and privacy issues for these apps.

Requirements: For many of these apps the identification of the user/vehicle may not be a strict requirement, even if a mechanism to (anonymously) authenticate the vehicles and possibly provide rewarding for collaboration is needed. Note that this analysis positions this category as similar to the one of participatory sensing, with the important difference that in this case data are often distributed locally in a peer-to-peer fashion, while in the other case data are usually first collected and then processed by a central entity.

2.6. Smart home and smart grid applications (SH–SG)

Characteristics: Homes and appliances within homes are being equipped with all sorts of sensors, mainly for safety and automation purposes, and smartphones are often used to run the applications based on the collected data. Energy consumption monitoring is being introduced by power companies mostly to facilitate billing but also with the goal of optimizing resources. Energy monitoring can act as another powerful source of data, very much like sensors.

Privacy threats and adversaries: The data collected in a home by sensors and by energy monitoring can reveal information about the people living in the home, their number, their habits in terms of activities they do in the home, when they usually are out and when they are in. For many people this is not information to be shared. Adversaries are the people outside the family, possibly including the power company or the home automation service provider as well as the entities they share the data with.

Requirements: All the people living in the home should be well aware of which kind of data is collected, in which rooms, what is locally processed and what is revealed externally to the providers. A flexible and user friendly method for privacy

Please cite this article in press as: C. Bettini, D. Riboni, Privacy protection in pervasive systems: State of the art and technical challenges, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.09.010

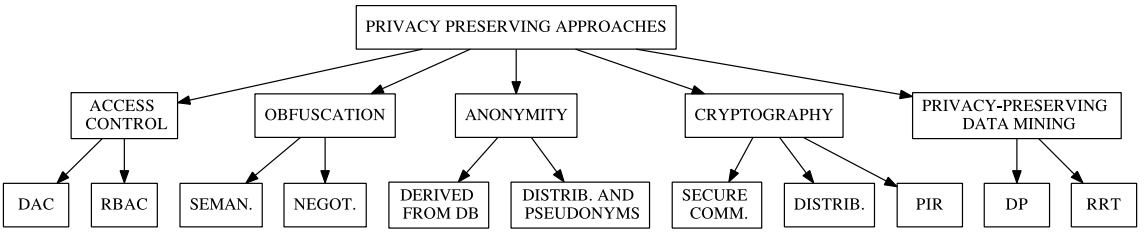

Fig. 1. Categorization of privacy preserving approaches for pervasive systems.

preference specification must be provided. The information released to external entities (e.g., the power company) must be at the maximum possible granularity (e.g. power consumption data may be aggregated in time intervals), possibly finding an acceptable tradeoff between privacy and the economical advantages of providing detailed information. Anonymity is unlikely to be acceptable for these apps since home address and owner's name are used for billing.

2.7. Common requirements

In addition to the specific requirements identified above for the different application categories, we identify a common set of requirements.

- Transparency and minimization. A distinguishing feature of pervasive computing is to embed sensing technology into everyday objects; this can lead to invisible data collection and use. A first requirement is for the users to be aware of the data they are sharing. This includes to know when sensors are active, which kind of data are collected, who is receiving them and what is done with them. In principle, a good regulation should impose to the entities that collect sensitive data to make them available to the owner; possibly providing different levels of abstraction (from raw data to higher-level inferred data), through a user-friendly interface as well as automatically through APIs. In any case, the collector should clearly state which kind of analyses it performs on the data and how the data are used. If it releases the data to third parties, it should specify which data are given to which entity. Finally, minimization should be considered since the design of the application: only personal data that is strictly needed should be collected.
- Privacy preference specification. Personal data sensitivity is in general subjective and context-dependent; hence, formalisms and tools are needed to facilitate the specification of preferences. In order to enable informed decisions, we can envision automatic reasoning tools to evaluate which higher-level data can be inferred by joining personal information obtained by different data collectors. Before releasing new data, or granting access to new entities, the system may notify the user about the additional data that could be inferred.
- Protection. Despite not being mentioned, communication of sensitive data should always be protected by some form of encryption. However, this covers only the communication channel; privacy protection mechanisms are needed to enforce the user's privacy policies. The appropriate privacy mechanism depends on the assumed adversary model and must also be designed to achieve an acceptable trade-off between privacy and its costs in terms of overhead in the use of resources and in terms of the service precision. Protection techniques relying on anonymity or pseudonymity would greatly benefit from advanced identity management systems.

3. Privacy preserving approaches

With respect to the identified requirements, in this section we focus on the most prominent approaches to privacy protection, while the other two common requirements identified above will be discussed in Section 4.

The considered approaches are illustrated in Fig. 1. We provide an executive summary below, in order to summarize the most commonly adopted approaches for each application category, as well as the different architectural models.

3.1. Executive summary

Based on our investigation, Table 2 recaps the most commonly applied approaches for each application category that we have considered in our study.

As illustrated in Table 3, most approaches support the *on the fly* provision of sanitized context data at the time of service request. However, approaches based on privacy-preserving data mining (i.e., PPDM-DP and PPDM-RRT) can be applied only to the offline release of sensitive data. Anonymity methods derived from DB privacy notions (ANON-DB) can be applied on the fly, possibly with the introduction of a small delay when temporal cloaking is used.

Table 4 illustrates how the different approaches protect against the disclosure of the sensitive association between a user's identity and sensitive data. The marker '+' appears when the technique protects the release of that part of the association. For example, anonymity methods, as well as differential privacy techniques, avoid the disclosure of users' identity. Anonymity does it by modifying identity information while differential privacy by applying statistical perturbations on sensitive data. Cryptographic methods protect sensitive data but some of them also protect identity (indicated by marker '∼').

Please cite this article in press as: C. Bettini, D. Riboni, Privacy protection in pervasive systems: State of the art and technical challenges, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.09.010

Table 2
Commonly adopted privacy preserving approaches for application categories.

App category	Approaches
LBS, MA, GeoSNs	DAC, RBAC, OBF-SEM, OBF-NEGOT, ANON-DB, ANON-D&P, CRYPT-SC, CRYPT-PIR, PPDM-DP
PS	DAC, ANON-D&P, CRYPT-DIST, PPDM-RRT
HC–WB	DAC, RBAC, ANON-DB, CRYPT-DIST
VA–SC	ANON-D&P

Table 3
On the fly vs. offline approaches.

	On the fly	Offline
DAC	+	−
RBAC	+	−
OBF-SEM	+	−
OBF-NEGOT	+	−
ANON-DB	∼	∼
ANON-D&P	+	−
CRYPT-SC	+	−
CRYPT-DIST	+	−
CRYPT-PIR	+	−
PPDM-DP	−	+
PPDM-RRT	−	+

Table 4
Protection against the disclosure of the sensitive association.

	Identity	Sensitive data
Access control	−	+
Obfuscation	−	+
Anonymity	+	−
Cryptography	∼	+
PPDM-DP	+	−
PPDM-RRT	−	+

Table 5
Architectural model of privacy preserving approaches.

	Client–server	Trusted third party	Distributed
DAC	+	−	−
RBAC	+	−	−
OBF-SEM	+	+	−
OBF-NEGOT	+	−	−
ANON-DB	−	+	+
ANON-D&P	−	+	+
CRYPT-SC	+	−	+
CRYPT-DIST	−	+	+
CRYPT-PIR	+	−	−
PPDM-DP	−	+	−
PPDM-RRT	+	−	−

From an architectural point of view, Table 5 shows the different models that can be adopted to implement the considered approaches.

3.2. Access control to private information

The problem of access control consists in deciding whether to grant or deny a given entity (*subject*) the right to perform a given *action* on a given resource (*object*). For the sake of this paper, we assume that the object is a user's private information, while the subjects are service providers, infrastructure components, or other users, wanting to acquire a user's personal context data. Access control techniques have been thoroughly studied in the field of databases, operating systems, and distributed systems. However, pervasive systems have peculiar features, which claim for specific access control methods. In particular, authorizations often depend on contextual conditions; hence, the access control system must take into account the continuously changing context of the involved entities.

Different context-aware access control techniques have been proposed, which adopt different approaches. In *discretionary* access control (DAC) [9] methods, authorizations depend (among other things) on the identity of the subject, while in *role-based* access control (RBAC) [10] they depend on the role of the subject within a structured organization. In

Please cite this article in press as: C. Bettini, D. Riboni, Privacy protection in pervasive systems: State of the art and technical challenges, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.09.010

mandatory access control (MAC) systems, a sensitivity level is assigned to each object, and policies define which sensitivity levels each subject is allowed to access. While the DAC approach is well suited to unstructured domains (e.g., generic Internet services), RBAC is more appropriate for structured domains, like companies and hospitals, since the use of functional roles simplifies the definition of access control policies. The MAC approach is well suited to domains in which the private information can be naturally organized in a hierarchy of sensitivity levels.

In the following, we describe relevant context-aware access control methods based on DAC and RBAC, which are the most widely used approaches in pervasive systems.

Techniques derived from DAC. Even early approaches to DAC allowed the expression of conditions to constrain permissions on the basis of the spatial and temporal characterization of the subject [11]. For instance, in a bank setting, an access control policy could be stated, granting access to customer accounts to authorized personnel only during working hours and from hosts within the bank. However, pervasive systems claim for more sophisticated DAC methods and languages to express complex conditions on multiple and continuously changing context data, as proposed by Hull et al. in [12] and by Pigeot et al. in [13]. Atluri and Shin in [14] presented an access control system specifically addressed to the preservation of mobile customers privacy. Customers can express policies controlling the release of private data based on spatio-temporal context and preferences. For instance, a user could state a policy to disclose her location and profile information only during the weekend and if she is in a mall, and only in exchange for a discount coupon on items in her shopping list. An efficient intermediary infrastructure is in charge of managing context data and preferences of mobile customers, and of enforcing their privacy policies.

More recently, Behrooz and Devlic proposed in [15] a context-aware DAC system to express privacy policies, which allows to control the granularity of released information. The policy language supports the definition of complex situations by means of an ontology-based context model, and supports the expression of social relationships, as well as temporal conditions.

The *SensorSafe* context-aware access control system, proposed by Chakraborty et al. in [16], specifically targets the release of personal sensor data. Privacy policies may consider a wide range of context data, including time, location, physiological parameters, and activities, as well as the entity requesting the data. The level of disclosure of personal sensor data is chosen by a broker, based on trust among users and subjects. Sensor data are obfuscated to diminish their sensitivity: in particular, location and timestamps are generalized, and sets of raw sensor data are abstracted to *context labels*, such as "stressed", "noise", "conversation".

Other methods adopt *secret authorization* mechanisms to certify the data provided by the subject (e.g., private context data), without revealing either the private information of the subject, or the private authorization policies of the object owner. This approach is pursued by Hengartner and Steenkiste in [17] through the use of access-rights graphs and hidden constraints, and by Wang et al. in [18] through the *zero-knowledge proof theory* [19]

Techniques derived from RBAC. Many other proposals for context-aware access control are based on extensions of the RBAC model with *dynamic* roles, possibly changing based on context. That approach has been followed by the *UbiCOSM* middleware [20]. The context model of UbiCOSM distinguishes between the *physical* dimension, which considers the presence of users in a specific location, and the *logical* dimension, which describes higher-level data such as the user's current activity. For instance, the context *TouristAtMuseum* is composed of the physical context *AtMuseum* (characterized by the presence of the user within the physical boundaries of a museum) and by the logical context *Tourist* (which defines the user's role as the one of a tourist). Rules are specified using an RDF-based language.

More recently, a context-aware RBAC system for the healthcare domain has been proposed by Poulymenopoulou et al. in [21]. In that system, private patients data are stored in the cloud, and a context manager is in charge of mediating between subjects and objects. The context model is based on OWL [22] ontologies, while privacy policies are expressed in the SWRL [23] language. Both permanent and temporary roles are supported; for instance, in an emergency situation, the staff member having permanent role "ambulance driver" may assume the temporary role "supporting attendant staff".

Semantic Web technologies are used also by Shen in [24] to represent context-aware privacy policies, as well as the users' context and role. Policies can take into account the social context, including proximity with other people, task-related activities, and social relationships.

Remarks. The main strong point of techniques derived from DAC consists in the efficiency of their reasoning procedures. On the other hand, techniques derived from RBAC can be profitably exploited not only in structured organizational domains but also in open environments, provided that they are supported by the possibility to handle dynamic and temporary roles. Nevertheless, challenging research issues remain open. An evident weakness of most of the existing systems lies in their rigidity: access to a given information is either granted or denied. A more flexible mechanism could be achieved by the use of obfuscation techniques, in order to disclose the required data at different levels of granularity, possibly considering trust, as done in [16]. As a final remark, we point out that access control methods do not protect privacy when the access to a service is private information by itself.

3.3. Obfuscation of private information

Most existing access control systems either grant or deny access to a given context data depending on the current situation. This "all or nothing" approach is not always the best choice, since denying context data may determine the impossibility

Please cite this article in press as: C. Bettini, D. Riboni, Privacy protection in pervasive systems: State of the art and technical challenges, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.09.010

to take advantage of a context-aware service. A more flexible solution can be achieved by coupling access control mechanisms with *obfuscation* [25] of the private data before its disclosure. The intuition beyond obfuscation is that each private data is associated to a given sensitivity level, which depends on the accuracy of the information itself: in general, the less the information is accurate, the less it is sensitive.

Obfuscation is usually achieved by generalizing the information, or providing fake information. For instance, consider a pervasive service suggesting venues to visit based on the current activity of users. Suppose that a user is traveling abroad for a job interview, and that the service is only partially trusted by the user. In this case, the current activity *JobInterview* is a very precise private information that the user does not want to disclose. However, she can still take advantage of the service by providing the obfuscated activity *Working*.

There has been extensive research on location obfuscation, well described in a survey by Jensen et al. [26]. In this section, we focus on extensions of those methods to support context data. The main research issue in this field is to devise techniques to provide adequate privacy preservation while retaining the usefulness of the data to context-awareness purposes, possibly by means of negotiation between users and service providers.

Semantic obfuscation methods (OBF-SEM). One of the first systems for release of obfuscated context data is the *semantic eWallet*, proposed by Gandon and Sadeh in [27]. Users of that system could express their preferences about the accuracy level of context data based on the requester's identity and on the context of the request. In particular, obfuscation preferences are represented by rules, whose preconditions express contextual conditions, and postconditions express the obfuscated context data to be released. That system supports both generalization and falsification of context data. A limitation of this approach is that the obfuscation conditions must be explicitly stated for each possible instantiation of context data.

A more general approach to obfuscation preference modeling has been proposed by Wishart et al. in [28]. That work is based on an ontological representation of context data, organized as nodes into a hierarchy, such that parent nodes represent more general concepts with respect to their children. For instance, the node *SocialActivity* may have two children nodes *BusinessMeeting* and *FriendlyMeeting*; the latter may have children nodes *TeamSport* and *BirthdayParty*, and so on. Users can express their obfuscation preferences, deciding the obfuscation level to apply to a context data based on the context of the request; for instance, "*disclose the current activity with accuracy at granularity level 2 to friends during the weekend*". A similar proposal has been presented by Rahman et al. in [29], and applied to an activity-aware instant message system. In that work, a trusted third party is in charge of context reasoning and enforcement of obfuscation policies.

Negotiation of obfuscation directives (OBF-NEGOT). In many cases, user's obfuscation preferences may conflict with service providers requirements in terms of *quality of context information* (QoC). In order to address this issue, Sheikh et al. in [30] propose a method to negotiate the quality of released context data between the user and the service provider. QoC is expressed in terms of five indicators: precision, freshness, spatial and temporal resolution, and probability of correctness. The service provider declares its requirements in terms of QoC, while the user specifies her policies about the maximum quality level for each indicator that she is willing to provide to access the service. If service provider requirements and user's policies are not incompatible, an intermediary layer is in charge of finding the most appropriate combination of quality levels of the indicators.

Multimodal sensing is more and more adopted to support ambient assisted living applications. Of course, audio/video streams, as well as other sensor data acquired within a home, carry very sensitive data about the occupants; hence specific techniques must be adopted to control their release to third parties. Moncrieff et al. in [31] propose a method to adapt privacy policies according to the current context of a home inhabitant, including location, anxiety and hazard conditions, activity and social context. Policies are extracted through a decision tree algorithm based on a training set, and determine the granularity level of data to be released. Dynamic data obfuscation methods are proposed by Moncrieff et al. in [32] also to enforce privacy protection in public surveillance systems.

Privacy preservation for exchange of context data among a group of people involved in a common social activity is addressed by Franz et al. in [33]. Before sharing data among them, the group members negotiate a privacy policy, defining which context data are needed for the social activity, and at which level of accuracy. Then, context data of the individuals are privately merged by a trusted infrastructure, in order to derive the social context of the group, without revealing the private context data of its members. For instance, given the exact locations of the participants, the infrastructure can derive the centroid of the group. With this method, the privacy guarantees strongly depend on the reasoning methods used by the infrastructure to derive the social context.

Remarks. Being coupled with hierarchical context models, semantic obfuscation methods simplify the definition of obfuscation directives by means of granularity levels. However, the specificity level of a context data in the context model may not always correspond to its sensitivity level. Moreover, while this approach is well suited to categorical context data that may be naturally represented by hierarchies, it is less suited to data in continuous domains, like physical location, physiological parameters, and so on.

Negotiation-based methods address the problem of choosing the more appropriate trade-off between privacy preferences of users and application requirements. However, it is still possible that a service requires context data at an accuracy level that the user is not willing to disclose: in that case, the service cannot be used. In order to overcome this issue, anonymization techniques (presented in Section 3.4) have been proposed, which protect from the disclosure of the user's identity, while possibly providing accurate context information.

Please cite this article in press as: C. Bettini, D. Riboni, Privacy protection in pervasive systems: State of the art and technical challenges, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.09.010

3.4. Anonymity

In several pervasive computing applications it is not strictly necessary to know the identity of users. For instance, participatory sensing applications and vehicular applications generally do not rely on the identity of people providing sensed context data, and many context-aware Internet services do not require authenticated access. For these applications, anonymity techniques are very appealing privacy preserving methods. The goal of anonymity methods is essentially to avoid that released context data may be used by an adversary to re-identify the data source. In participatory sensing and vehicular applications, anonymity techniques are coupled with reputation mechanisms for assessing the trust level of anonymous sources. A challenging issue is how to enable anonymous authentication. Different EU projects have tackled this topic. In particular, PrimeLife[3] addressed the definition of a platform for privacy-conscious identity managements. The *identity mixer* (idemix)[4] system adopts cryptographic primitives to provide *anonymous credentials*, which allow an individual to prove claimed attributes (e.g., age) to a third party, without revealing his/her identity.

Techniques derived from database anonymity notions (ANON-DB). In the area of database systems, the notion of k-anonymity has been introduced by Samarati in [34]. The goal of k-anonymity is to guarantee that each released record can be associated to at least k possible respondents. In order to enforce anonymity it is necessary to determine which attributes in a table play the role of *quasi-identifiers (QI)*, i.e., data that joined with external knowledge may help the adversary to restrict the set of possible respondents. Techniques for database anonymization usually assume a user-trusted data curator, which generalizes *QI* values and/or suppresses records, in order to guarantee that each record is indistinguishable by at least other $k-1$ records based on the value of the QI attributes. A set of records indistinguishable based on their QI values is called a *QI-group*. Since each individual is assumed to be the respondent of a single record, if each record belongs to a QI-group of at least k records, there are at least k candidate respondents for each released record. Other anonymity notions have been proposed, including l-diversity [35] and t-closeness [36], in order to overcome different weaknesses of k-anonymity.

The notion of k-anonymity has been applied to different context-aware systems. In location-based services (LBS), an adversary having access to (even approximate) users' location may be able to identify the issuer of a request based on its spatio-temporal parameters. Hence, several works have applied anonymity methods to LBS [37,38], by generalizing the precise location data in a request to an area including a sufficiently large set of other potential issuers. However, many other context data besides location may be used by an adversary to identify the issuer of a request. Hence, following that approach, a large amount of context data should be generalized in order to enforce anonymity. As a result, the context information released to a service provider could be too coarse to provide the service at an acceptable quality level. In order to limit the information loss due to the generalization of context data, four different personalized anonymization models are proposed by Shin et al. in [39]. These models allow a user to constrain the maximum level of location and profile generalization still guaranteeing the desired level of anonymity. For instance, a user could decide to constrain the maximum level of location generalization to an area of 1 km^2, while imposing no constraints on the level of generalization of her profile.

A further issue to be considered is the defense against the well-known problem of *homogeneity* [35] identified in the field of databases. Homogeneity attacks can be performed if all the records belonging to a QI-group have the same value of sensitive information. In this case it is clear that the adversary may easily violate the users' privacy despite anonymity being formally enforced. The same problem may arise as well in context-aware services in the case an adversary recognizes that all the potential issuers actually issued a request with the same value of private information. A proposal to defend against such attacks in context-aware systems has been presented by Riboni et al. in [40]. That proposal aims at protecting from multiple-issuers historical attacks by generalizing both context data and service parameters.

Well-being applications generally rely not only users' location, but on many other context data, such as users' activities. This fact enables novel kinds of privacy attacks, like the one presented by Riboni et al. in [41]. In that work, it is shown that even enforcing k-anonymity, an attacker may be able to recognize the actual issuer of a service request to a well-being application by monitoring the behavior of the potential issuers with respect to service responses. For example, consider a pervasive system of a gym, suggesting exercises on the basis of gender, age, and physiological data retrieved from body-worn sensors. Even if users are anonymous in a set of k potential issuers, the attacker can easily recognize the issuer of a particular request if she starts to use in a reasonable lapse of time a machine the system suggested to her, which was not suggested to any other potential issuer. The solution proposed in [41] relies on an intermediary trusted entity that filters all the communications between users and service providers, calculates the probability of privacy violations corresponding to possible alternatives suggested by the service (e.g., the next exercise to perform), and notifies the user, so that she can take an informed decision.

However, we point out that any privacy protection method derived from database anonymity notions provides formal privacy guarantees only under strict assumptions about the background knowledge available to possible adversaries: if the actual adversarial knowledge is different than assumed by the defender, the identity of the data respondents may be easily reconstructed.

Distributed approaches and use of pseudonyms (ANON-D&P). Other privacy-preserving methods aim at enforcing anonymity without assuming the existence of a centralized user-trusted data curator. Shin et al. proposed the *AnonySense* [42] system

[3] http://primelife.ercim.eu/.
[4] http://www.zurich.ibm.com/security/idemix/.

Please cite this article in press as: C. Bettini, D. Riboni, Privacy protection in pervasive systems: State of the art and technical challenges, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.09.010

for anonymous participatory sensing. In AnonySense, user's anonymity is enforced by routing sensed information through multiple servers, which insert random delays and aggregate the measurements provided by different users, such that the aggregated context information cannot be used by an adversary to identify the users. If a user communicates her data to an untrusted intermediate server, obfuscation methods and techniques derived from database anonymity notions can be applied.

A different method for privacy protection in participatory sensing application was proposed by Boutsis and Kalogeraki in [43]. In particular, they tackle a system to share users' trajectories. They propose a distributed architecture, in which trajectory points are secretly distributed across the mobile devices of a community of users, such that each user knows only a small part of the trajectories of any other user. With that method, the trajectory information available to each user should be insufficient to identify the source of the trajectory. Different kinds of spatio-temporal queries can be distributively answered, without revealing the identities of contributing users. However, this defense is prone to attacks when multiple malicious users collude to reconstruct a trajectory, which could be used to re-identify its source.

Even if a participatory sensing application does not rely on users' identity, it may benefit from considering the reputation of the anonymous sources. Hence, Christin et al. in [44] proposed a framework to anonymously certify the reputation score of users contributing context data to participatory sensing applications. The anonymization method is based on the use of pseudonyms, which are associated to cloaked reputation levels. The user's pseudonym is periodically changed, and cryptographic *blind signatures* [45] are used by an application server to verify the reputation of the source, without revealing the identity of the individual. Of course, that framework does not protect against adversaries trying to re-identify the user based on the provided context data.

An anonymous accountability mechanism for vehicular applications is proposed by Raya et al. in [46]. The mechanism relies on a tamper-proof device, installed on the vehicle, which keeps a set of anonymous keys provided by a certification authority. Each key has a short lifetime and expires after its usage; hence, different messages cannot be linked and attributed to the same vehicle. In case the vehicle communicates false information, the certificate authority can reconstruct the vehicle identity based on the used key, and revoke its keys.

Other techniques for enforcing anonymity and security in participatory sensing and vehicular applications are reviewed in [5,8], respectively.

Remarks. Anonymity methods protect not only against the release of private context information, but also when the access to a context-aware service is the sensitive information to protect by itself. Techniques derived from database anonymity notions provide formal privacy guarantees according to a given adversary model. However, quantifying the external knowledge available to possible adversaries is very difficult in practice. If wrong assumptions are made (i.e., if the adversary has different knowledge than the assumed one), an adversary may be able to identify the data source, even if anonymity methods are formally enforced. Moreover, methods derived from database anonymity notions assume the existence of a user-trusted data curator in charge of anonymizing the data; this poses trust issues, and may result in a single point of failure when the data must be anonymized on the fly. Different distributed approaches do not require the existence of a centralized user-trusted server, since anonymization is demanded to multiple intermediary servers, or to the client nodes themselves. In some cases, specific methods are proposed to take into account the reputation of nodes through the use of pseudonyms. While not relying on a trusted third party is a clear advantage in terms of trust, those methods provide less formal guarantees, since they may be prone to attacks from malicious nodes.

3.5. Cryptography and private information retrieval

Cryptographic primitives have been extensively used to secure wireless communication of sensitive context data in pervasive system, to privately perform distributed computations, and to enforce confidentiality of both service parameters and responses.

Secure communications (CRYPT-SC). The use of wireless channels, and more generally insecure channels, poses a first threat for users' privacy, since it makes easier for an adversary to acquire service requests and responses by eavesdropping the communication or analyzing traffic on the network. Two natural countermeasures are: (a) implement secure communication channels so that no third party can obtain requests/responses while they are in transit, and (b) avoid the recognition of the client's network address, even by the service provider, which may be untrusted.

Onion Routing [47] implements both the features of IP hiding and message encryption. In order to preserve the sender's IP address, each message travels towards the receiver via a series of proxies, called *onion routers*, which choose the next component of the path setting an unpredictable route. Each router in the path removes one encryption level from the message before forwarding it to the next router.

Multi-party and distributed cryptographic protocols (CRYPT-DIST). Different cryptographic protocols have been designed to distributively answer queries, such as "compute the pollution level in the center of Milano", without revealing the identity of participants. Even if the computation of the measure of interest is performed in a distributed fashion, those protocols generally rely on centralized entities to broadcast queries, or to distribute cryptographic tokens.

De Cristofaro and Soriente proposed the *PEPSI* [48] system for privacy-preserving participatory sensing. In PEPSI, a registration authority is in charge of providing cryptographic authorization tokens to queriers and to mobile nodes communicating their sensitive context data. Each sensing task is identified by a label; e.g., "*Temperature in Manhattan, New York*". The *identity-based encryption* [49] (IBE) cryptographic primitive is used to associate public and private keys to each sensing task.

Please cite this article in press as: C. Bettini, D. Riboni, Privacy protection in pervasive systems: State of the art and technical challenges, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.09.010

In particular, IBE allows to compute the public key of an entity by solely knowing the entity's ID. Since each sensing task is identified by its label, mobile nodes can compute the public key of their tasks without relying on complex public-key infrastructures and certification authorities. Mobile nodes encrypt their readings using the public key of the label corresponding to their sensing task, and provide them to the service provider, which sends them to the queriers that subscribed to that task. Queriers decrypt the readings using the private key obtained by the registration authority.

Commutative encryption schemes are used by Mascetti et al. in [50] for proximity notifications in GeoSNs.

Regarding the app category VA–SC, the use of homomorphic encryption has been proposed by Garcia and Jacobs in [51] for secure and privacy-preserving smart metering. Homomorphic encryption is used to compute aggregated consumption at the neighboring level, without revealing the consumption of any individual household. Frauds can be detected by comparing the computed aggregated measurement with the actual consumption at the neighboring level.

Private information retrieval (CRYPT-PIR). Cryptographic techniques can also be used to hide from the service provider the exact request parameters, as well as the response. This approach has been proposed in the area of LBS where location information is often considered sensitive by users. In particular, solutions based on this approach usually aim at retrieving the nearest neighbor (NN) point of interest with respect to the user position at the time of the request. A first solution was proposed by Atallah and Frikken in [52]: the authors propose a form of encrypted query processing combining the use of a data structure suited for managing spatial information with a cryptographic schema for secret sharing. On the server side, location data are handled through a directed acyclic graph, whose nodes correspond to Voronoi regions obtained by a tessellation of the space with respect to points of interest stored by the service provider. The query processing is performed according to the protocol proposed by Atallah and Du in [53], which allows a client to retrieve the correct Voronoi area without communicating its precise location. The drawback of this solution is that, in order to resolve an NN query, the user needs to send a number of queries that is proportional to the depth of the graph instead of a single request.

More recently, a cryptographic approach was proposed by Ghinita et al. in [54]. The service provider builds a Voronoi tessellation according to the stored points of interest, and superimposes on its top a regular grid of arbitrary granularity. In order to obtain the response to an NN query, the privacy preservation mechanism relies on a private information retrieval technique that is used for encrypting the user query, and for retrieving part of the location database without revealing spatial information. Some of the strong points of this solution are that location data are never disclosed; the user's identity is confused among identities of all users; and no trusted third party is needed to protect the users' privacy. However, since mobile devices are often characterized by limited computational capability, the query encryption and the answer processing performed at the client side have a strong impact on service response time, network and power consumption. In particular, when applied to context-aware services that perform the adaptation on a wide set of heterogeneous context data, this technique may result in unacceptable computation overhead both at the client and at the server side.

Remarks. There exist well-established cryptographic techniques to secure point-to-point communications of sensitive context data from the source to a trusted recipient. When the recipient is untrusted, more complex distributed architectures, such as onion routing, can be used to achieve a limited form of anonymity. However, secure communication methods may not enforce anonymity when the message contains information that, matched with background knowledge, may allow an adversary to restrict the set of possible sources. In order to protect against that threat, anonymity techniques should be enforced.

Similarly, distributed cryptographic protocols may not enforce anonymity when the adversary has background knowledge. Even when anonymity is not a requirement, as in the medical emergency scenario considered in [55], cryptographic methods may not be sufficient to protect users' privacy. For instance, using the system proposed in [55], an adversary could reconstruct the exact location of a doctor by submitting multiple fictitious queries from random fake locations: when a doctor communicates that it is in close proximity to a given location, her private information is directly revealed. These kinds of attacks could be avoided by coupling cryptographic methods with obfuscation of the sensitive data.

Private information retrieval techniques offer strong privacy guarantees, since they avoid the application server from knowing not only the request parameters, but even its own response. However, in general they incur high overhead in terms of computational and communication costs; hence, they are feasible only for a limited set of applications.

3.6. Privacy-preserving data mining

The unprecedented quantity of digital data traces that people leave as they go about their everyday lives is more and more exploited by data miners to understand the trends and dynamics of today's society. Most of the contextual "big data" acquired from pervasive systems involve the private sphere of individuals. Hence, several efforts have been made to apply privacy-preserving data mining (PPDM) methods to data acquired from pervasive systems that must be released to third parties for analysis.

Differential privacy (PPDM-DP). A PPDM technique that gained wide popularity in the last few years is differential privacy (DP) [56]. Essentially, in the DP approach, a user-trusted data curator releases sanitized statistics about sensitive data gathered from a set of individuals, guaranteeing that an adversary cannot reconstruct the original micro-data by observing the statistics. In particular, DP ensures that the probability distribution of released statistics does not significantly change, irrespective of whether the data of a single individual is present in or absent from the original knowledge base. This property is enforced by adding random noise in a principled way to the exact statistics.

Please cite this article in press as: C. Bettini, D. Riboni, Privacy protection in pervasive systems: State of the art and technical challenges, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.09.010

DP has been recently applied by Riboni and Bettini in [57] to the problem of releasing private check-ins data to an untrusted third-party. In that system, a trusted check-in collector is in charge of applying DP to check-in statistics before releasing them to an untrusted recommender system. That method protects against both the recommender system, and its users, who may issue fictitious queries to the system in order to reconstruct the places visited by a target individual. Hardt and Nath in [58] present a distributed protocol for achieving DP in a mobile advertising application, in which users' preferences are derived from private context data. That protocol is intended to maximize the trade-off among privacy, efficiency and effectiveness of ad delivery.

Applications of differential privacy to billing based on smart meter readings are illustrated by Barthe et al. [59]. The strong point of DP methods is that they do not rely on assumptions about the external knowledge available to adversaries; moreover, in general they are computationally efficient, since noise is randomly extracted from standard probability distributions. However, the utility of released statistics strongly depends on the number of individuals contributing their data: if too few data are available, the sanitized statistics has very little utility, since the magnitude of noise is of the same order of magnitude of the true data.

Randomized response techniques (PPDM-RRT). Alternative PPDM methods include randomized response techniques (RRT) [60] to release *discrete* sensitive data. In RTT, the data owner randomly perturbs the true micro-data before releasing it to an untrusted data collector. The data is perturbed according to a probabilistic function known by the data collector. When the collector has received a sufficient amount of data from the owners, it can infer an approximation of the probability distribution function of the data, without being able to reconstruct the individual micro-data. *Negative surveys* are a particular class of RRT, in which the released value is chosen with uniform probability among the fake values.

Groat et al. in [61] apply the negative survey method to multidimensional categorical data acquired from a participatory sensing system. The strong points of that solution is that it does not rely on computationally expensive cryptographic protocols, and it does not assume the existence of a trusted data curator. However, finding the most appropriate trade-off between privacy and data utility with this method is not simple. On the one hand, the achieved privacy level increases with the number of possible values. On the other hand, the more numerous the possible values, the less accurate the reconstructed data. Moreover, this method is prone to background knowledge attacks. A similar approach is used by Xing et al. in [62] to reconstruct data from participatory sensing applications, through data transformation and aggregation at the participatory nodes, and regression model fitting.

Remarks. The PPDM approach can be used for applications relying on statistical data, like recommender systems, social behavior mining, and participatory sensing. Differential privacy methods offer strong privacy guarantees, irrespective of the background knowledge available to an adversary. However, they assume the existence of a trusted data curator. Randomized response techniques do not rely on trusted third parties, but are prone to background knowledge attacks, and they may not always provide an appropriate trade-off between the achieved privacy guarantees and data accuracy. Moreover, the data utility provided by PPDM methods is strongly related to the magnitude of available data.

4. Open issues and research challenges

From the many privacy violation accidents that we have been witnessing in the last years it is clear that, on one side, the large amount of research done on privacy protection is not yet making it to the products, and, on the other side, it seems that a solution to the problem of privacy probably goes beyond the implementation of an effective technique. To make the problem even more difficult, privacy breaches may also result from security holes in the design of the operating system and other software equipping our devices, as illustrated for mobile phone applications in recent work [63]. Clearly, in this case the privacy protection approaches we are considering are not effective.

In this section, we describe what we believe are the major challenges we will be facing in the near future to address or at least mitigate the privacy problem. Our focus is clearly on pervasive applications, but most challenges actually hold in a general context.

4.1. Technical challenges

Referring to the requisites we have identified and to the existing techniques presented in Section 3 the following are topics that deserve further investigation.

- Transparency and monitoring tools. Very limited efforts have been done in this direction with respect to what is needed. The reader interested in a state-of-the-art on this topic can refer to results from a recent EU project addressing these aspects as well as identity management (PrimeLife[5]) and to a recent Ph.D. dissertation [64]. However, we will probably see effective tools that can integrate and intuitively present the information about an individual held by different providers only when new regulations will be in place, as elaborated in the legal aspects below.
- Integration of different methods to achieve a good trade-off between privacy, efficiency, and quality of service. We believe that a promising direction is the combination of methods based on recent advances in cryptography (e.g., efficient private

5 http://primelife.ercim.eu/.

Please cite this article in press as: C. Bettini, D. Riboni, Privacy protection in pervasive systems: State of the art and technical challenges, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.09.010

set intersection and private set union [65]), and obfuscation based methods, with the goal of balancing efficiency and effectiveness. This combination has been recently applied for private proximity notification [50].

- Data utility. Reconciling users' privacy preferences with the data utility needed by service providers is a major challenge for any privacy-preserving solution. Ideally, only the data that is strictly needed to provide the service at a satisfactory quality level should be disclosed, avoiding the release of unnecessary data to untrusted parties. This direction is followed by Chakraborty et al. in [16], who propose the use of a broker and trust-based methods. A different technique to reconcile privacy and data utility has been proposed by Massaguer et al. in [66]; in that work, privacy is modeled as the negative utility deriving from the release of a piece of information, and a distributed simulated annealing algorithm is used to maximize the utility of information released to the service provider while enforcing the user's privacy preferences.
- A major challenge that remains is the accurate modeling of the adversary knowledge that in some cases is hardly predictable. Very conservative assumptions can lead to overprotective techniques with high costs and insufficient service precision, while privacy violations may occur if the adversary has access to more external knowledge than assumed. Examples of this last case abound in the literature.

Since privacy is a multi-faceted topic we are fully aware that there are many other aspects to be considered. In the following we briefly mention some of them.

4.2. User experience aspects and challenges

User experience plays a major role both in the definition of what is considered sensitive information, and in the actual adoption of privacy enhancing technology. Regarding the first issue, we should not forget that the introduction of Kodak cameras raised similar issues than the ones Google Glass is generating now. The perception of what can be shared, and with whom, changes for different individuals depending on their current context, social status, and many other factors. This is especially true if we consider that we have almost no experience yet with pervasive applications. Hence, a first challenge is to provide flexible protection mechanisms that can adapt to the actual privacy preferences of individuals and to deal with their evolutions. A second challenge is how to capture these preferences without forcing the user to go through complex settings of system parameters whose consequences they can hardly understand [67].

The availability of transparency and monitoring tools is probably a prerequisite for the user to be aware of a potential privacy threat and hence to express a preference. In addition we believe there are two promising research directions: the first is the automatic or guided identification of privacy preferences. Existing techniques are generally based on user-friendly interfaces to define a set of if-then-else rules. However, this method may be tedious, or even too complicated for the average users. An intriguing alternative is to automatically infer the privacy policies based on statistical analysis of the past decisions of the user, as done by Zhang et al. in [68] using rough set theory. An interesting direction in this sense may be developing personalized privacy assistants capable of engaging in dialogs with users to help them semi-automatically evaluate privacy policies and configure privacy settings.

The second is a consequence based policy specification framework. In this case, the user is more explicitly involved in the specification of the polices, but it takes decisions with the support of a tool that illustrates the consequences of making different privacy choices [69]. This is somehow related to the monitoring tools cited above.

4.3. Legal aspects and challenges

Based on what happened in the last 10 years, it is very likely that privacy protection technology alone cannot win the battle against the uncontrolled massive release and misuse of personal data that technology itself is enabling. For example, designing an effective and popular privacy-aware GeoSN mobile application requires the GeoSN service provider to specifically support privacy oriented APIs. Designing a useful monitoring app showing in an aggregated and user friendly form which personal information the user has released up to now requires server side support: service providers and data collectors should offer APIs so that individuals through dedicated apps can selectively and automatically retrieve their personal information. Without a proper regulation it seems unlikely that this will happen on a large scale any time soon. The risk is that no matter how we improve the privacy protection techniques illustrated in Section 3, the great majority of users will still be subject to disastrous privacy breaches. The principles of *privacy by default*, *right to be forgotten*, *right to transfer personal data* and the more general *privacy by design* contained in recent proposals for new regulations[6] are a promising step in this direction. The challenge will be to have regulations including these principles approved worldwide, and most importantly making industry actually comply. An interesting overview on this issue is presented by Mulligan et al. [70].

4.4. Economic aspects and challenges

There are at least two main obstacles to the widespread adoption of privacy protection technology. First, the actual implementation by industry of the legal principles mentioned above is likely to have costs far superior to what firms

[6] http://ec.europa.eu/justice/data-protection/.

Please cite this article in press as: C. Bettini, D. Riboni, Privacy protection in pervasive systems: State of the art and technical challenges, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.09.010

currently spend for having their lawyers draft and update privacy notices. For example, being able to automatically and selectively delete or release through APIs personal historical data may require redesigning or at least revising the firm information system. Even higher costs are required to actually implement the *privacy by design* principle. If privacy is to be considered in the technical design, development and testing of the products, new professional figures need to be hired with skills on the topics we surveyed in Section 3 and working closely with social scientists, ethicists, and HCI experts. Some large IT companies have already taken this road, but the majority will probably hardly do it without proper incentives and new regulations. The second obstacle is due to the incompatibility between some of the current business models and the reduced personal information that some of the privacy protection techniques impose. For example, there are technological solutions to effectively notify smartphone users of the proximity of their friends that avoid revealing any information about the location of the user and of their friends to the service provider. However, one of the asset values of the provider for this kind of service is actually the user location and movements, possibly for a mobile advertisement service or for building and selling marketing profiles. This suggests as one of the challenges that privacy engineers should design protection schemes that still enable profitable business models and that providers also need to adapt by devising new or adapted business models.

For completeness, there are also studies in the field of economics of privacy that question the advantage of offering more transparency and control to the users. Based on some experiments it is argued that control might paradoxically increase riskier disclosure by soothing privacy concerns, while transparency might be easily muted, and its effect even arbitrarily manipulated [71].

5. Conclusions

In this paper we analyzed the privacy issues arising from the use of current mobile and pervasive applications. By grouping applications in a few main categories, we identified both common and specific requirements, and presented a description of the main privacy protection approaches.

We have also briefly discussed the challenges due to the many inter-disciplinary aspects of data privacy that cannot be ignored for devising an effective solution: they include relevant social, economic, and legal challenges. Our work is inevitably incomplete, due to the vast existing literature on data privacy and security, to the multi-faceted problem of data privacy, and, most importantly to the rapidly changing world of pervasive applications of which all of us are just witnessing its early stage of evolution. Nevertheless, we hope that our contribution can be useful especially to young researchers and pervasive application designers to acquire awareness about the privacy problem and of the main approaches that have been proposed to alleviate it, as well as to inspire ideas for new research directions.

References

[1] L. Ackerman, Mobile health and fitness applications and information privacy—report to california consumer protection foundation, Tech. Rep., Privacy Rights Clearinghouse, 2013.
[2] J. Cas, Ubiquitous computing, privacy and data protection: options and limitations to reconcile the unprecedented contradictions, in: S. Gutwirth, Y. Poullet, P.D. Hert, R. Leenes (Eds.), Computers, Privacy and Data Protection: an Element of Choice, Springer, 2011, pp. 139–169.
[3] C. Bettini, S. Jajodia, P. Samarati, X.S. Wang (Eds.), Privacy in Location-Based Applications, Research Issues and Emerging Trends, in: Lecture Notes in Computer Science, vol. 5599, Springer, 2009.
[4] M. Wernke, P. Skvortsov, F. Dürr, K. Rothermel, A classification of location privacy attacks and approaches, Pers. Ubiquitous Comput. 18 (1) (2014) 163–175.
[5] D. Christin, A. Reinhardt, S.S. Kanhere, M. Hollick, A survey on privacy in mobile participatory sensing applications, J. Syst. Softw. 84 (11) (2011) 1928–1946.
[6] M. Kranz, A. Möller, N.Y. Hammerla, S. Diewald, T. Plötz, P. Olivier, L. Roalter, The mobile fitness coach: towards individualized skill assessment using personalized mobile devices, Pervasive Mob. Comput. 9 (2) (2013) 203–215.
[7] K. Michael, M.G. Michael, No limits to watching? Commun. ACM 56 (11) (2013) 26–28.
[8] J. Domingo-Ferrer, Q. Wu, Safety and privacy in vehicular communications, in: C. Bettini, S. Jajodia, P. Samarati, X.S. Wang (Eds.), Privacy in Location-Based Applications, Research Issues and Emerging Trends, in: Lecture Notes in Computer Science, vol. 5599, Springer, 2009, pp. 173–189.
[9] R. Sandhu, P. Samarati, Access control: principles and practice, IEEE Commun. 32 (9) (1994) 40–48.
[10] R.S. Sandhu, E.J. Coyne, H.L. Feinstein, C.E. Youman, Role-based access control models, IEEE Comput. 29 (2) (1996) 38–47.
[11] C. Bettini, Temporal access control, in: Encyclopedia of Cryptography and Security, second ed., Springer, 2011, pp. 1284–1285.
[12] R. Hull, B. Kumar, D. Lieuwen, P. Patel-Schneider, A. Sahuguet, S. Varadarajan, A. Vyas, Enabling context-aware and privacy-conscious user data sharing, in: Proceedings of the 2004 IEEE International Conference on Mobile Data Management, (MDM'04), IEEE Computer Society, 2004, pp. 187–198.
[13] C.-E. Pigeot, Y. Gripay, V.-M. Scuturici, J.-M. Pierson, Context-sensitive security framework for pervasive environments, in: Proceedings of the Fourth European Conference on Universal Multiservice Networks, (ECUMN 2007), IEEE Computer Society, 2007, pp. 391–400.
[14] V. Atluri, H. Shin, Efficient security policy enforcement in a location based service environment, in: Proceedings of Data and Applications Security XXI, 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security, in: Lecture Notes in Computer Science, vol. 4602, Springer, 2007, pp. 61–76.
[15] A. Behrooz, A. Devlic, A context-aware privacy policy language for controlling access to context information of mobile users, in: Security and Privacy in Mobile Information and Communication Systems (MobiSec), in: Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 94, Springer, 2012, pp. 25–39.
[16] S. Chakraborty, Z. Charbiwala, H. Choi, K.R. Raghavan, M.B. Srivastava, Balancing behavioral privacy and information utility in sensory data flows, Pervasive Mob. Comput. 8 (3) (2012) 331–345.
[17] U. Hengartner, P. Steenkiste, Avoiding privacy violations caused by context-sensitive services, Pervasive Mob. Comput. 2 (3) (2006) 427–452.
[18] C.-D. Wang, L.-C. Feng, Q. Wang, Zero-knowledge-based user authentication technique in context-aware system, in: Multimedia and Ubiquitous Engineering, 2007. MUE'07. International Conference on, 2007, pp. 874–879.
[19] S. Goldwasser, S. Micali, C. Rackoff, The knowledge complexity of interactive proof systems, SIAM J. Comput. 18 (1) (1989) 186–208.
[20] A. Corradi, R. Montanari, D. Tibaldi, Context-based access control management in ubiquitous environments, in: Proceedings of the 3rd IEEE International Symposium on Network Computing and Applications, (NCA 2004), IEEE Computer Society, 2004, pp. 253–260.

Please cite this article in press as: C. Bettini, D. Riboni, Privacy protection in pervasive systems: State of the art and technical challenges, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.09.010

[21] M. Poulymenopoulou, F. Malamateniou, G. Vassilacopoulos, An access control framework for pervasive mobile healthcare systems utilizing cloud services, in: Wireless Mobile Communication and Healthcare, in: Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 83, Springer, 2011, pp. 380–385.
[22] I. Horrocks, P.F. Patel-Schneider, F. van Harmelen, From SHIQ and RDF to OWL: the making of a web ontology language, J. Web Sem. 1 (1) (2003) 7–26.
[23] I. Horrocks, P.F. Patel-Schneider, H. Boley, S. Tabet, B. Grosof, M. Dean, SWRL: a Semantic Web rule language combining OWL and RuleML, W3c member submission, W3C (May 2004). URL: http://www.w3.org/Submission/2004/SUBM-SWRL-20040521/.
[24] H. Shen, A semantic context-based access control model for pervasive computing environments, in: Advances in Computer Science and Information Engineering, in: Advances in Intelligent and Soft Computing, vol. 168, Springer, 2012, pp. 135–140.
[25] D.E. Bakken, R. Parameswaran, D.M. Blough, A.A. Franz, T.J. Palmer, Data obfuscation: anonymity and desensitization of usable data sets, IEEE Secur. Privacy 2 (6) (2004) 34–41.
[26] C.S. Jensen, H. Lu, M.L. Yiu, Location privacy techniques in client–server architectures, in: C. Bettini, S. Jajodia, P. Samarati, X.S. Wang (Eds.), Privacy in Location-Based Applications, Research Issues and Emerging Trends, in: Lecture Notes in Computer Science, vol. 5599, Springer, 2009, pp. 31–58.
[27] F.L. Gandon, N.M. Sadeh, Semantic web technologies to reconcile privacy and context awareness, J. Web Sem. 1 (3) (2004) 241–260.
[28] R. Wishart, K. Henricksen, J. Indulska, Context privacy and obfuscation supported by dynamic context source discovery and processing in a context management system, in: Proceedings of the 4th International Conference on Ubiquitous Intelligence and Computing, (UIC 2007), in: Lecture Notes in Computer Science, vol. 4611, Springer, 2007, pp. 929–940.
[29] F. Rahman, M.E. Hoque, F.A. Kawsar, S.I. Ahamed, User privacy protection in pervasive social networking applications using PCO, Int. J. Soc. Comput. Cyber-Phys. Syst. 1 (3) (2012) 242–267.
[30] K. Sheikh, M. Wegdam, M. van Sinderen, Quality-of-context and its use for protecting privacy in context aware systems, J. Softw. 3 (3) (2008) 83–93.
[31] S. Moncrieff, S. Venkatesh, G.A.W. West, Dynamic privacy assessment in a smart house environment using multimodal sensing, ACM Trans. Multimedia Comput. Commun. Appl. 5 (2) (2008).
[32] S. Moncrieff, S. Venkatesh, G.A.W. West, Dynamic privacy in public surveillance, IEEE Comput. 42 (9) (2009) 22–28.
[33] E. Franz, T. Springer, N. Harder, Enhancing privacy in social applications with the notion of group context, in: 7th International Conference for Internet Technology and Secured Transactions, IEEE, 2012, pp. 112–118.
[34] P. Samarati, Protecting respondents' identities in microdata release, IEEE Trans. Knowl. Data Eng. 13 (6) (2001) 1010–1027.
[35] A. Machanavajjhala, J. Gehrke, D. Kifer, M. Venkitasubramaniam, *l*-diversity: privacy beyond *k*-anonymity, in: Proceedings of ICDE 2006, IEEE Computer Society, 2006.
[36] N. Li, T. Li, S. Venkatasubramanian, *t*-closeness: privacy beyond *k*-anonymity and *l*-diversity, in: Proceedings of ICDE 2007, IEEE Computer Society, 2007, pp. 106–115.
[37] M. Gruteser, D. Grunwald, Anonymous usage of location-based services through spatial and temporal cloaking, in: Proc. of the 1st International Conference on Mobile Systems, Applications and Services (MobiSys), USENIX Association, 2003, pp. 31–42.
[38] B. Gedik, L. Liu, Protecting location privacy with personalized *k*-anonymity: architecture and algorithms, IEEE Trans. Mob. Comput. 7 (1) (2008) 1–18.
[39] H. Shin, V. Atluri, J. Vaidya, A profile anonymization model for privacy in a personalized location based service environment, in: Proceedings of the 9th International Conference on Mobile Data Management (MDM'08), 2008, pp. 73–80.
[40] D. Riboni, L. Pareschi, C. Bettini, S. Jajodia, Preserving anonymity of recurrent location-based queries, in: Proceedings of the 16th International Symposium on Temporal Representation and Reasoning (TIME), IEEE Computer Society, 2009, pp. 62–69.
[41] D. Riboni, L. Pareschi, C. Bettini, Shadow attacks on users' anonymity in pervasive computing environments, Pervasive Mob. Comput. 4 (6) (2008) 819–835.
[42] M. Shin, C. Cornelius, D. Peebles, A. Kapadia, D. Kotz, N. Triandopoulos, Anonysense: a system for anonymous opportunistic sensing, Pervasive Mob. Comput. 7 (1) (2011) 16–30.
[43] I. Boutsis, V. Kalogeraki, Privacy preservation for participatory sensing data, in: 2013 IEEE International Conference on Pervasive Computing and Communications, PerCom 2013, San Diego, CA, USA, March 18–22, 2013, IEEE Computer Society, 2013, pp. 103–113.
[44] D. Christin, C. Roßkopf, M. Hollick, L.A. Martucci, S.S. Kanhere, Incognisense: an anonymity-preserving reputation framework for participatory sensing applications, Pervasive Mob. Comput. 9 (3) (2013) 353–371.
[45] D. Chaum, Blind signatures for untraceable payments, in: Advances in Cryptology: Proceedings of CRYPTO'82, Plenum Press, New York, 1982, pp. 199–203.
[46] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, J.-P. Hubaux, Eviction of misbehaving and faulty nodes in vehicular networks, IEEE J. Sel. Areas Commun. 25 (8) (2007) 1557–1568.
[47] D. Goldschlag, M. Reed, P. Syverson, Onion routing, Commun. ACM 42 (2) (1999) 39–41. http://doi.acm.org/10.1145/293411.293443.
[48] E.D. Cristofaro, C. Soriente, Extended capabilities for a privacy-enhanced participatory sensing infrastructure (pepsi), IEEE Trans. Inf. Forensics Secur. 8 (12) (2013) 2021–2033.
[49] D. Boneh, M.K. Franklin, Identity-based encryption from the weil pairing, in: Proceedings of the 21st Annual International Cryptology Conference, in: Lecture Notes in Computer Science, vol. 2139, Springer, 2001, pp. 213–229.
[50] S. Mascetti, D. Freni, C. Bettini, X.S. Wang, S. Jajodia, Privacy in geo-social networks: proximity notification with untrusted service providers and curious buddies, VLDB J. 20 (4) (2011) 541–566.
[51] F.D. Garcia, B. Jacobs, Privacy-friendly energy-metering via homomorphic encryption, in: Proceedings of Security and Trust Management—6th International Workshop, in: Lecture Notes in Computer Science, vol. 6710, Springer, 2011, pp. 226–238.
[52] M.J. Atallah, K.B. Frikken, Privacy-preserving location-dependent query processing, in: ICPS'04: Proceedings of the The IEEE/ACS International Conference on Pervasive Services, IEEE Computer Society, 2004, pp. 9–17.
[53] M.J. Atallah, W. Du, Secure multi-party computational geometry, in: WADS'01: Proceedings of the 7th International Workshop on Algorithms and Data Structures, Springer-Verlag, London, UK, 2001, pp. 165–179.
[54] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, K.-L. Tan, Private queries in location based services: anonymizers are not necessary, in: Proceedings of the ACM SIGMOD International Conference on Management of Data, (SIGMOD 2008), ACM, 2008, pp. 121–132.
[55] P.S. Efraimidis, G. Drosatos, F. Nalbadis, A. Tasidou, An efficient privacy-preserving solution for finding the nearest doctor, Pers. Ubiquitous Comput. 18 (1) (2014) 75–90.
[56] C. Dwork, Differential privacy, in: Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, (ICALP'06), in: Lecture Notes in Computer Science, vol. 4052, Springer, 2006, pp. 1–12.
[57] D. Riboni, C. Bettini, Differentially-private release of check-in data for venue recommendation, in: Proceedings of the 2014 IEEE International Conference on Pervasive Computing and Communications (PerCom), IEEE Computer Society, 2014, pp. 190–198.
[58] M. Hardt, S. Nath, Privacy-aware personalization for mobile advertising, in: ACM Conference on Computer and Communications Security, ACM, 2012, pp. 662–673.
[59] G. Barthe, G. Danezis, B. Grégoire, C. Kunz, S.Z. Béguelin, Verified computational differential privacy with applications to smart metering, in: Proceedings of the 26th Computer Security Foundations Symposium, IEEE, 2013, pp. 287–301.
[60] W. Du, Z. Zhan, Using randomized response techniques for privacy-preserving data mining, in: Proceedings of the Ninth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, ACM, 2003, pp. 505–510.
[61] M.M. Groat, B. Edwards, J. Horey, W. He, S. Forrest, Application and analysis of multidimensional negative surveys in participatory sensing applications, Pervasive Mob. Comput. 9 (3) (2013) 372–391.
[62] K. Xing, Z. Wan, P. Hu, H. Zhu, Y. Wang, X. Chen, Y. Wang, L. Huang, Mutual privacy-preserving regression modeling in participatory sensing, in: Proceedings of the IEEE INFOCOM 2013, IEEE, 2013, pp. 3039–3047.

Please cite this article in press as: C. Bettini, D. Riboni, Privacy protection in pervasive systems: State of the art and technical challenges, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.09.010

[63] X. Zhou, S. Demetriou, D. He, M. Naveed, X. Pan, X. Wang, C.A. Gunter, K. Nahrstedt, Identity, location, disease and more: Inferring your secrets from android public resources, in: Proceedings of the 2013 ACM SIGSAC Conference on Computer %26; Communications Security, CCS'13, ACM, New York, NY, USA, 2013, pp. 1017–1028. http://doi.acm.org/10.1145/2508859.2516661.
[64] T. Pulls, Privacy-preserving transparency-enhancing tools (Phd Dissertation) Karlstad University, 2012.
[65] E. De Cristofaro, G. Tsudik, Experimenting with fast private set intersection, in: Trust and Trustworthy Computing, in: Lecture Notes in Computer Science, vol. 7344, Springer, 2012, pp. 55–73.
[66] D. Massaguer, B. Hore, M.H. Diallo, S. Mehrotra, N. Venkatasubramanian, Middleware for pervasive spaces: balancing privacy and utility, in: Proceedings of Middleware 2009, ACM/IFIP/USENIX, 10th International Middleware Conference, in: Lecture Notes in Computer Science, vol. 5896, Springer, 2009, pp. 247–267.
[67] M. Benisch, P.G. Kelley, N.M. Sadeh, L.F. Cranor, Capturing location-privacy preferences: quantifying accuracy and user-burden tradeoffs, Pers. Ubiquitous Comput. 15 (7) (2011) 679–694.
[68] Q. Zhang, Y. Qi, J. Zhao, D. Hou, T. Zhao, L. Liu, A study on context-aware privacy protection for personal information, in: Proceedings of the 16th IEEE International Conference on Computer Communications and Networks, (ICCCN 2007), IEEE Computer Society, 2007, pp. 1351–1358.
[69] Z. Benenson, A.D. Luca, S. Fischer-Hübner, J. Meyer, Consequence-based privacy decisions: a new way to better privacy management, 'My Life, Shared'—trust and privacy in the age of ubiquitous experience sharing (Dagstuhl Seminar 13312) 3 (7).
[70] D.K. Mulligan, K.A. Bamberger, What regulators can do to advance privacy through design, Commun. ACM 56 (11) (2013) 20–22. http://doi.acm.org/10.1145/2527185.
[71] A. Acquisti, I. Adjerid, L. Brandimarte, Gone in 15 s: the limits of privacy transparency and control, IEEE Secur. Privacy 11 (4) (2013) 72–74.

Please cite this article in press as: C. Bettini, D. Riboni, Privacy protection in pervasive systems: State of the art and technical challenges, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.09.010