The Pursuit of Citizens' Privacy: A Privacy-Aware Smart City Is Possible

Antoni Martínez-Ballesté, Pablo A. Pérez-Martínez, and Agusti Solanas,
Universitat Rovira i Virgili

ABSTRACT

Cities are growing steadily, and the process of urbanization is a common trend in the world. Although cities are getting bigger, they are not necessarily getting better. With the aim to provide citizens with a better place to live, a new concept of a city was born: the smart city. The real meaning of smart city is not strictly defined, but it has gained much attention, and many cities are taking action in order to be considered "smart." These smart cities, founded on the use of information and communication technologies, aim at tackling many local problems, from local economy and transportation to quality of life and e-governance. Although technology helps to solve many of these local problems, their ability to gather unprecedented amounts of information could endanger the privacy of citizens. In this article we identify a number of privacy breaches that can appear within the context of smart cities and their services. We leverage some concepts of previously defined privacy models and define the concept of citizens' privacy as a model with five dimensions: identity privacy, query privacy, location privacy, footprint privacy and owner privacy. By means of several examples of smart city services, we define each privacy dimension and show how existing privacy enhancing technologies could be used to preserve citizens' privacy.

INTRODUCTION

Countries struggle to be competitive, attract investments and talent, reduce debt, and be globally sustainable. Due to factors related to economies of scale, many services are more easily provided in highly populated areas. Hence, people are moving from the country to the cities, and a urbanization trend is beginning to be apparent throughout the world. As a result of this urbanization process, cities are gaining importance, and their role as economic engines is becoming more prominent nationally and also at an international level.

The struggle of countries for competitiveness has a smaller counterpart in the shape of their cities. Those cities are internationally competing for investments, talent, and even to increase tourism, and they realize that the most promising path to success requires the use of technology. Thanks to information and communication technologies (ICT), local governments and private companies like Cisco and IBM are developing and implementing innovative solutions to improve the management of cities' operations in a variety of areas: namely transportation, energy, sustainability, e-governance, economy, communications, and so on.

Although the concept of a smart city is pretty new, we can find several examples of cities that have adopted it. For example, the city of Amsterdam [1] has defined four areas (i.e., sustainable living, sustainable working, sustainable mobility, and sustainable public space) around the idea of sustainability, in which smart projects are conducted in order to improve the city and transform it into a real smart city in the near future. In Amsterdam, they focus on the reduction of CO_2 emissions, but there are other approaches focused on reducing the cost of public services and transportation [2], improving the interaction of the society with the administration, or simply improving the experience of tourists. Some other examples of cities working along the "smart" line are Vienna, Toronto, Paris, New York, London, Tokyo, Copenhagen, Hong Kong, and Barcelona [3].

The fundamental rights of citizens should be guaranteed at all times. In this regard, for smart cities to be a successful reality, we emphasize the importance of the preservation of privacy. Most of the services offered in smart cities are based on ICT. Users interact with these services through a wealth of devices (e.g., smartphones, information kiosks, public computers) that are connected using heterogeneous networks and systems, which are the perfect target for attackers and eavesdroppers willing to disclose sensitive information from individuals or even to impersonate them. In addition, the huge amount of data collected and managed paves the way to the Big Brother effect. As a result, citizens might refrain from using smart city services to avert such problems.

Legislation is essential to guarantee the achievement of privacy within smart cities. Individuals must be aware of the ability of smart cities to silently gather a variety of information about them. Hence, the wide adoption of legislation regarding the collection and processing of personal data [4] within a smart city would be the icing on the cake.

This work was partly funded by the Spanish Government through project CONSOLIDER INGENIO 2010 CSD2007-0004 "ARES," project TSI2007-65406-,C03-01 "E-AEGIS," project TIN2011-27076-C03-01 "CO-PRIVACY," and by the Government of Catalonia under grant 2009 SGR 1135. The authors are with the UNESCO Chair in Data Privacy, but the views expressed in this article are their own and do not commit UNESCO. The third author is grateful for the financial support of the Spanish Ministry of Education, Culture and Sport with the José Castillejo Grant CAS0200/2012.

0163-6804/13/$25.00 © 2013 IEEE

Last but not least, although technical solutions (encryption, digital signatures, server reliability, etc.) make smart city services feasible from a security point of view, there is still a lot of work to be done to materialize the notion of privacy in smart cities.

In this article, we present the concept of Citizens Privacy, which consists in the application of the so-called Privacy Enhancing Technologies (PET) in the smart city scenario. We show that a combination of these techniques — currently used in privacy models for databases and location-based services —, can be applied to build a model for Citizens Privacy.

Background on Privacy Models

In this section, we recall two privacy models that can be applied to achieve citizens' privacy: the 3DConceptual Framework for Database Privacy [5] and the Where, Who, What (W^3) privacy model for location-based services (LBS) [6]. Figure 1 illustrates the theoretical privacy dimensions described in this section.

The 3D Conceptual Framework for Database Privacy

An astonishing amount of data from multiple sources is collected and stored in databases belonging to multiple parties (i.e., governments, private companies, etc.). The privacy of the data stored in these databases might be understood differently depending on the context and the operations applied. Domingo-Ferrer [5] splits database privacy issues into three dimensions related to the main actors involved: respondents, users, and owners.

Respondent privacy. This is focused on avoiding the re-identification of individuals (i.e., respondents) whose information is stored in a database.In the example of Fig. 1, the user queries an LBS provider and publishes his activities on social networks. These data are stored in the databases of the service providers and can be analyzed to obtain a variety of information. Regarding respondent privacy, no sensitive or private information should be leaked from these databases. They must be protected before being published or released to third parties. Statistical disclosure control (SDC) is usually used to do so.

User privacy. This is about guaranteeing the privacy of the queries made by a user to a database system (e.g., Internet search engines, LBS providers). The point is to obtain the desired information without revealing the real query to the database system. This is known as the private information retrieval (PIR) problem. In relation to our example, the queries made by the user to the LBS provider should follow a protocol to prevent the provider from learning them.

Owner privacy. This privacy dimension refers to the owner of a database queried by other users/entities. The owner might agree to share some of her data, but it should be controlled so that only those data (and no more) are gathered by the issuers of the queries. The privacy preserving data mining (PPDM) discipline designs techniques to address this problem. In our example, a third party (a data warehousing facility) pays an LBS provider and a social network to mine their data. In this case protecting owner privacy means to allow the third party to access the information he paid for but no more.

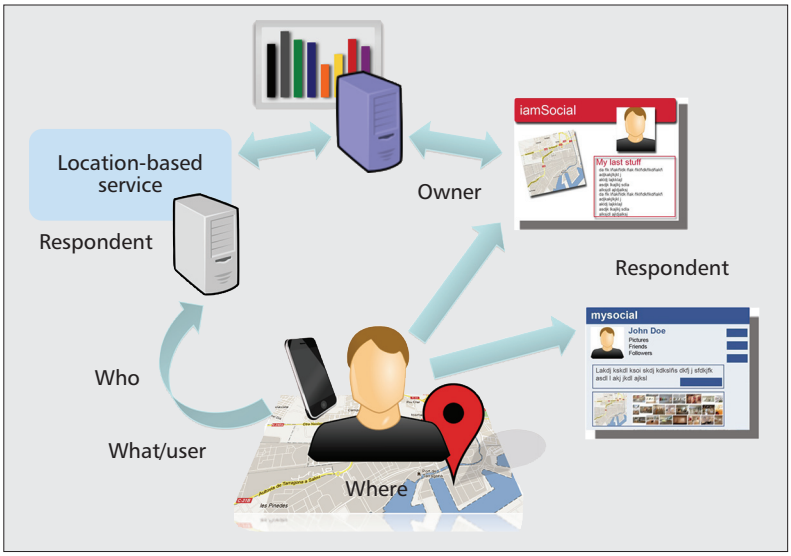

Figure 1. *Conceptual scheme of the privacy models. In the picture we distinguish (i) a user (at the bottom) who contacts a location-based service provider, (ii) two social networks (on the right) to which the user belongs, and (iii) a data warehousing facility (at the top).*

The aforementioned techniques (SDC, PIR, and PPDM) are described next.

W^3 Privacy for Location-Based Services

Services related to the location of the user are gaining importance, and so are privacy issues related to them. In [6] Pérez and Solanas describe the three dimensions of user privacy in LBS and define the concept of W^3 privacy. Those dimensions can be inferred from the main parts of a typical location-based query: "**Someone** is asking for **something** near **somewhere**":

Where. This is the privacy dimension related to the location of the user. LBS providers might learn that location from the queries of the user. Thus, users could be tracked. In our example, the user sends his current location to the LBS provider to obtain an answer. Thus, the LBS provider may track her. Several techniques have been proposed to mitigate this problem (collaborative location obfuscation, cloaking, etc.).

What. In general, LBS providers inform users about *something*. The *what* dimension of privacy in LBS refers to the privacy of the queries. Note that this dimension is very similar to the *user privacy* dimension in the database context. Hence, PIR techniques can also be used to approach it.

Who. This problem is about identifying the user and relating her with a bunch of queries. This might allow the provider to create user profiles. In order to mitigate this privacy issue, most solutions rely on intermediate entities to hide real identities using, for example, temporal pseudonyms.

The authors of [6] affirm that an LBS is W^3 private if the service is given while the LBS provider cannot know: who is the user, where is the user, and what the user asks for.

Researchers, practitioners, and administrators must take into account the privacy concerns that entail the pervasive nature of ICT in smart cities. To that end, we propose the concept of citizen privacy: a five-dimensional model for citizens' privacy in smart cities.

Privacy Enhancing Techniques for Citizens' Privacy

In this section, we describe the techniques that can be used in our citizens' privacy model: statistical disclosure control (SDC) , private information retrieval (PIR), privacy-preserving data mining (PPDM), location privacy, anonymity and pseudonyms, privacy in radio frequency identification (RFID), and privacy in video surveillance. Their use is illustrated in the example addressed later.

Statistical Disclosure Control — Private companies and statistical agencies collect data from people on a daily basis. On one hand, it is necessary to guarantee the right of the society to information but, on the other hand, the right to individual privacy should be preserved. The field of SDC aims to protect the privacy of individual respondents while allowing the release of their data for secondary use. Many techniques have been proposed to protect respondents' privacy (noise addition, microaggregation, rank swapping, rounding, etc.) [7]. The main aim of these techniques is to distort data in order to avoid the linkage of private information with individual respondents. At the same time, the distortion introduced into the data should be limited to preserve data utility. All in all, statistical disclosure control techniques try to find the right balance between information loss and disclosure risk. These topics are addressed and formalized under the methodologies of differential privacy [8].

Private Information Retrieval — Consider the problem in which party A wants to obtain a piece of information from a database belonging to another party, B. A wants that information but it does not want B to know which it is. This problem is known as the PIR problem; Chor, Goldreich, Kushilevitz, and Sudan introduced it in 1995 [9]. The simplest solution for A to achieve its goal is to ask B for the whole database. If B sends the database to A, it is impossible for B to know the information in which A is interested. However, this trivial solution is not practical due to communication costs. Since the problem was stated in 1995, a number of protocols have been proposed to reduce the computational and communication costs [10]. However, in general, PIR approaches are considered to be impractical in real scenarios yet.

Privacy-Preserving Data Mining — Due to the ability of ICT for gathering unprecedented amounts of data, data mining techniques gained much attention. The main goal of data mining is to develop models representing aggregated data so as to discover non-obvious, valuable data. More generally, we might say that data mining aims to obtain knowledge from data. However, due to numerous privacy concerns, data mining was seen as a privacy threat and the field of PPDM appeared to change data mining for the better, providing all its benefits while maintaining privacy [15]. In general, the PPDM problem can be seen as a game between two parties that do not trust each other. Both parties have some data and need to collaborate to obtain a common result, but they do not want to share their data. Many protocols have been proposed to approach this problem from simple data perturbation techniques to more sophisticated multiparty computation.

Location Privacy — When users try to obtain information from an LBS provider, they send their location and allow the LBS provider to track them. Several methods have been proposed to protect location privacy. Their aim is to provide a distorted location that prevents the provider from tracking users. In [12] the authors propose the use of a trusted third party (TTP), which handles users' locations to create cloaking regions. Users send these regions to the LBS, and since several users are under the same cloaking area, the server will not be able to correlate users and locations. Other proposals that do not rely on TTP also exist, but require several protocol rounds and/or users collaboration [13].

Anonymity and Pseudonyms — When users contact a service to obtain information, their identity is exposed to the provider, and it can link users with their queries (which might lead to profiling and thus invasion of privacy). To address this issue, most solutions rely on intermediate entities to hide the real identities of the users (e.g., using pseudonyms). Also, TTP-free versions based on collaboration among users have been proposed [14].

Privacy in RFID — RFID systems consist of tags and readers. Tags contain identification information of products that can be accessed by readers without the need for visual contact and cables. This is very convenient for the manufacturing sector, but might be a privacy problem if unauthorized people could read tags and obtain their confidential information (and by extension the information of the user). With the aim to solve this problem many protocols have been proposed, and it could be said that privacy and security can be guaranteed. However, the main problem is to achieve privacy and security in reasonable times (i.e., there are scalability problems) [15].

Privacy in Video Surveillance — Pervasive video surveillance systems inherently endanger the privacy of people: identities and activities can easily be retrieved from pictures and videos. People accept to be controlled for the sake of security, but most privacy advocates warn about the Big Brother effect. In [16], the authors claim that video surveillance systems must guarantee the private management of video data. To that end, they use real-time computer vision techniques to accurately detect regions of interest (i.e., faces, car plates, etc.), which are then protected.

A 5D Model for Privacy in Smart Cities

Researchers, practitioners, and administrators must take into account the privacy concerns that entail the pervasive nature of ICT in smart cities. To that end, we propose the concept of citizen's privacy, a five-dimensional model for citizens'

privacy in smart cities. The identified dimensions are: *identity* privacy, *query* privacy, *location* privacy, *footprint* privacy, and *owner* privacy. Next, we define each dimension in the context of a smart city. For each dimension, we show examples of privacy concerns. Also, we point to the technologies that could be used to address those concerns. The examples used throughout the section refer to Fig. 2. The goal of the scenario depicted in Fig. 2 is to provide a non-exhaustive but illustrative set of real smart city services. In the figure, we illustrate the following services.

Smart parking service. In this service, available parking spaces are controlled by sensors. Drivers are guided to the nearest available parking space, and they pay for the exact time that they use the parking space.

Electric car recharging. Complementing the parking service, electric cars can use recharging sockets. Users pay for the energy they consume to charge their cars.

Smart office building. This service controls who is in their office in order to optimize the energy consumption related to illumination, air conditioning, and so on.

Location-based service. This service allows the query of information based on the location of the requester. In our example, a citizen is looking for a list of nearby Italian restaurants.

Video surveillance system. For the sake of citizens' safety, the city is covered by a network of pervasive and interconnected cameras.

Smart bus service. This bus optimizes its route in real time according to the number of users that request its service.

Smart garbage containers. These containers send an alarm when they are full and need to be emptied. Moreover, only users living in the surrounding area can use them.

Control of power consumption at homes. In order to improve the production and distribution efficiency of energy, the consumption levels are collected via a sensor network.

Medical center. The medical center collects data from patients. Moreover, personnel in the medical center query other hospitals to retrieve information about the patients of whom they are in charge.

Interactive information pole. Users can access these devices to obtain information about the city. In addition, citizens identify themselves and access personalized services.

Our citizens' privacy model, including examples and solutions, is summarized in Table 1.

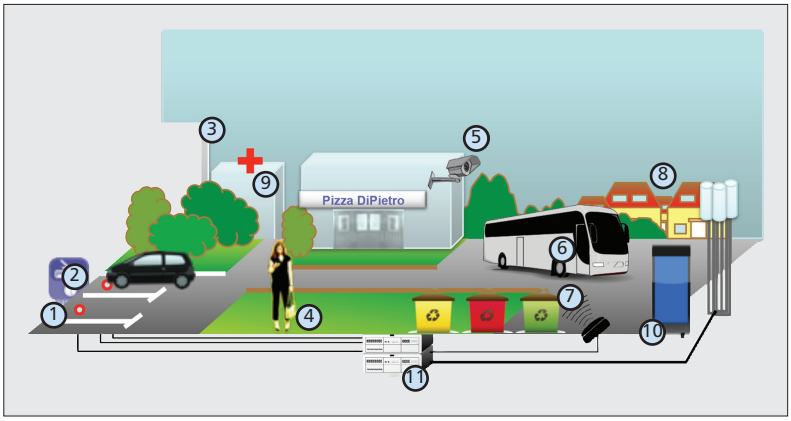

Figure 2. *Our example of smart city: (1) smart parking service; (2) electric car recharging; (3) smart building with control of presence; (4) user querying an LBS provider; (5) camera for video surveillance; (6) smart bus that changes the route based on users needs; (7) smart garbage containers; (8) control of energy consumption in homes; (9) medical center; (10) interactive information pole; (11) network infrastructure of the smart city.*

Identity Privacy

Definition — Identity privacy relates to disclosing the identity every time a user accesses a smart city service. In that sense, it is mapped to the Who privacy of the W^3 privacy model. If users specify their identity, service providers and other third parties will be able to correlate users and their activities.

Examples — This is a common issue in many services. Users disclose their identity when they access the smart parking service or pay for the car energy recharging service. Moreover, the detection of occupancy in the areas of the smart building could also entail identification. Also, as we have pointed out previously, the use of LBS generally entails identifying the user. Last but not least, the video surveillance system clearly involves identity privacy concerns.

Solution — The use of pseudonymizers contributes to preserve identity privacy. One could think of a single pseudonymizer service. However, if the service is attacked or their administrators misbehave, the relation between identities and pseudonyms can be disclosed. To avoid that situation, this service should be provided by a set of geographically distributed pseudonymizers. Finally, with regard to video surveillance, real-time accurate protection of the regions of interest might be applied.

Query Privacy

Definition — Query privacy is related to preserving the privacy of the queries made by users to services. Hence, it is mapped to both the user and what privacy dimensions. Upon collecting the queries made by users, service providers can profile users and obtain information about their habits.

Example — The interactive pole and the LBS involve this privacy issue. Moreover, services such as smart parking and smart bus may also entail query privacy, since the queries made by users can be analyzed to extract information about habits.

Solution — In general, PIR-like techniques might be used to mitigate the query privacy issue: services should include PIR tools that users might apply before querying the provider. Using TTP might also be an option. Whatever technique is applied, the goal should be hampering the correlation of users and queries.

Location Privacy

Definition — Location privacy is about guaranteeing that the privacy of the physical location of the user is preserved. This is the where dimension of the W^3 privacy model.

Our 5D approach	Mapping to existing models		Examples of privacy concerns	Existing solutions
	3D database	W3 LBS		
Identity		Who	Most of the examples entail identity privacy concerns. RFID and video surveillance are also related to identity issues.	Pseudonymizers, RFID privacy techniques, privacy-aware video surveillance
Query	User	What	Mainly location-based services, interactive information poles, etc.	Private Information Retrieval techniques, random pseudonymizers
Location		Where	Location-based services, other services involving location (for example, smart parking). Also video surveillance entails location privacy.	Collaboration for location masking, cloaking, pseudonymization, privacy-aware video surveillance
Footprint	Respondent		Microdata generated from a variety of sources (sensors, RFID readers, medical data, electronic voting, etc.)	Anonymization, Statistical Disclosure Control
Owner	Owner		Obtaining information across databases belonging to different entities.	Privacy-Preserving Data Mining, Statistical Disclosure Control

Table 1. *Summary of our 5D proposal for modeling the privacy aspects in smart city services.*

Example — Clearly, the LBS of our scenario entails location privacy issues. However, almost all the depicted services also entail them: using the smart parking service, users disclose their location in order to be routed to the nearest parking area; using the car recharging service, the location of a user's car is disclosed; the smart building is also aware of the location of individuals; and so on.

Solution — In some cases in which the location is not constant, LBS users could collaborate to mask their exact locations. Also, a cloaking service could be used to protect real locations.

Footprint Privacy

Definition — Footprint privacy is related to the control of the information that can be retrieved or inferred from microdata sets. Actually, the activities in a smart city involve the acquisition, collection and storage of large amounts of microdata (i.e., the information at the level of respondents). In our definition of footprint privacy, these microdata are obtained from a variety of sources, such as sensor networks and RFID readers. Hence, a service is related to a microdata set that records the information about the use of the service (i.e., the *footprint* of the users on the service). The microdata sets can be published or released to third parties, so the latter can obtain a variety of information. The privacy of individuals must be preserved; hence, the disclosure of sensitive information should not be possible from the released data. Therefore, this dimension can be mapped to the respondent dimension described for database privacy.

Example — All the services that involve the acquisition of information about their utilization may suffer from footprint privacy issues.

Solution — The aforementioned SDC techniques must be applied over the data sets before their release. Besides deleting the identification information (or at least replacing it by pseudonyms), some procedures should be performed to control the disclosure risk while restraining the information loss.

Owner Privacy

Definition — Owner privacy deals with the privacy-aware computation of queries across the databases from different autonomous entities. This dimension is directly borrowed from the owner dimension described for database privacy.

Example — Let us focus on energy consumption control in homes and assume that the electricity company wants to correlate the use of electricity with the use of other services such as telephony or gas. A naive solution would be that the telecommunications and gas companies release their footprint databases to the electricity company. Naturally, the knowledge extracted from these databases is highly attractive for strategic and commercial decisions; consequently, these companies may refrain from releasing or sharing their data.

Solution — The owner privacy issues are the natural scenario for PPDM techniques and even SDC. If they are applied to the queries across the databases, the amount of information actually transferred to the entity that originates the query will be controlled.

Conclusions

The concept of the smart city has been adopted by many cities in the world, and the challenge of being "smart" is gaining importance in the agenda of local governments. To be smart, cities must be sustainable, improve the quality of life of their citizens, foster their interaction through e-governance, and so on. To achieve these goals, local governments are making serious efforts to

move in the "smart direction," and private companies like IBM and Cisco are playing (and will play) a determinant role in the success of the smart cities of the future.

We believe that real smart cities count on their citizens, and they must protect their privacy to make this challenge a true success. In this article we have presented the concept of citizens' privacy. Our model distinguishes five dimensions: identity privacy, query privacy, location privacy, footprint privacy, and owner privacy. Also, we have identified a number of real-life situations that might jeopardize the privacy of the citizens of a smart city, and we have shown how to preserve it by using off-the-shelf privacy enhancing technologies.

The technologies we have proposed are feasible and could be implemented in any smart city. However, their success will depend on some inherent aspects that should be addressed. For instance, the coexistence of multiple infrastructure domains should be properly tackled, and the transportation of the information between these parts should be done in a secure manner. Moreover, companies offering data center services for the smart city infrastructure should take care of the security and reliability of their systems and networks. Finally, the adoption of security technologies in resource constrained devices — which is being solved thanks to the efforts of researchers and practitioners — must be also considered.

To achieve these goals, local governments are making serious efforts to move in the "smart direction," and private companies like IBM and Cisco are playing (and will play) a determinant role in the success of the smart cities of the future.

References

[9] B. Chor *et al.*, "Private Information Retrieval," *Proc. 36th Annual Symp. Foundations of Computer Science*, 1995, Oct. 1995, pp. 41–50.

[3] B. Cohen, "The top 10 Smart Cities on the Planet," http: //www.fastcompany.com, 2012; http://www.fastcoexist.com/1679127/ the-top-10-smart-cities-on-the-planet.

[4] EC, "Protection of Personal Data," http: //ec.europa.eu/justice/data-protection/index en.htm, 2013.

[5] J. Domingo-Ferrer, "A Three-Dimensional Conceptual Framework for Database Privacy," W. Jonker and M. Petkovic, Eds., *Secure Data Management*, *Lecture Notes in Computer Science*, vol. 4721, Springer, 2007, pp. 193–202.

[8] C. Dwork, "Differential Privacy," *ICALP: Annual Int'l. Colloquium on Automata, Languages and Programming,* 2006.

[12] B. Gedik and L. Liu, "Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms," *IEEE Trans. Mobile Computing*, vol. 7, Jan. 2008, pp. 1–18.

[7] A. Hundepool *et al.*, *Statistical Disclosure Control*, John Wiley & Sons, Ltd, 2012.

[2] IBM, Integrated Fare Management for Transportation, , 2011, http://www.ibm.com/smarterplanet/us/en/traffic/congestion/nextsteps/solution/G080151O85496M88.html.

[1] Liander and AIM, "Amsterdam Smart City," 2012, http://www. amsterdamsmartcity.nl/#/en.

[16] A. Martínez-Ballesté *et al.*, "Towards A Trustworthy Privacy in Pervasive Video Surveillance Systems," *IEEE PerCom Wksps.*, 2012, pp. 914–19.

[6] P. A. Pérez-Martínez and Agusti Solanas, "W3-privacy: the three dimensions of user privacy in LBS," *12th ACM Int'l. Symp. Mobile Ad Hoc Networking and Computing*, Paris, France, May 2011.

[14] P. A. Pérez-Martínez, A. Solanas, and A. Martínez-Ballesté, "Location Privacy through Users' Collaboration: A Distributed Pseudonymizer," *Proc. 2009 3rd Int'l. Conf. Mobile Ubiquitous Computing, Systems*, Services and Technologies,, 2009, pp. 338–41.

[15] A. Solanas *et al.*, "A Distributed Architecture for Scalable Private RFID Tag Identification," *Computer Networks*, vol. 51, no. 9, 2007, pp. 2268–79.

[13] A. Solanas and A. Martínez-Ballesté, "A TTP-Free Protocol for Location Privacy in Location-Based Services," *Computer Commun.*, vol. 31, no. 6, 2008, pp. 1181–91.

[11] J. Vaidya and C. Clifton, "Privacy-Preserving Data Mining: Why, How, and When," *IEEE Security Privacy*, vol. 2, no. 6, Nov.–Dec. 2004, pp. 19–27.

[10] X. Yi *et al.*, "Single-Database Private Information Retrieval from fully Homomorphic Encryption," *IEEE Trans. Knowledge and Data Engineering*, vol. PP, no. 99, 2012, p. 1.

Biographies

Antoni Martínez-Ballesté (antoni.martinez@urv.cat) is a tenured assistant professor in the Department of Computer Science and Mathematics at Universitat Rovira i Virgili (URV), Catalonia, Spain. He received his M.Sc. degree in Computer Engineering from URV in 2002. He obtained his Ph.D. in telematics engineering from Universitat Politècnica de Catalunya in 2004 with honours. His research interests include security and privacy aspects of information and communications technologies and their users. He has authored over 70 publications.

Pablo Alejandro Pérez Martínez (pabloalejandro.perez@urv.cat) is a predoctoral researcher at CRISES Research Group and the UNESCO Chair in Data Privacy in the Department of Computer Science and Mathematics at URV. He obtained his B.Sc. degree in computer science from the Universitat de Lleida, and his M.Sc. in computer science and Security from URV.

Agusti Solanas [M] (agusti.solanas@urv.cat) is a researcher at URV. He received his M.Sc. degree in computer engineering from URV in 2004 with honours (Outstanding Graduation Award). He received a Diploma of Advanced Studies (Master's) in telematics engineering from Universitat Politècnica de Catalunya in 2006 and a Ph.D. in telematics engineering from UPC in 2007 with honors. His main fields of activity are privacy and security. He has authored over 90 publications. He is a member of the ACM.