Preprint of
“Privacy in Mobile Participatory Sensing: Current Trends and Future Challenges”

By

Delphine Christin

Rheinische Friedrich-Wilhelms-Universität Bonn,
Friedrich-Ebert-Allee 144, 53113 Bonn, Germany
and
Fraunhofer FKIE, Fraunhoferstr. 20
53343 Wachtberg, Germany

E-Mail: christin@cs.uni-bonn.de
http://net.cs.uni-bonn.de/wg/ubips/

Accepted for publication in:
Journal of Systems and Software
DOI: 10.1016/j.jss.2015.03.067

Privacy in Mobile Participatory Sensing: Current Trends and Future Challenges

Delphine Christin[a,b]

[a] *Rheinische Friedrich-Wilhelms-Universität Bonn, Friedrich-Ebert-Allee 144, 53113 Bonn, Germany*
[b] *Fraunhofer FKIE, Fraunhoferstr. 20, 53343 Wachtberg, Germany*
E-Mail: christin@cs.uni-bonn.de

Abstract

Mobile participatory sensing has opened the doors to numerous sensing scenarios that were unimaginable few years ago. In absence of protection mechanisms, most of these applications may however endanger the privacy of the participants and end users. In this manuscript, we highlight both sources and targets of these threats to privacy and analyze how they are addressed in recent privacy-preserving mechanisms tailored to the characteristics of participatory sensing. We further provide an overview of current trends and future research challenges in this area.

Keywords: Mobile sensing, participatory sensing, privacy

1. Introduction

Mobile participatory sensing[1] takes advantage of the sensing, processing, and storage resources available in current mobile phones to gain insights about the participants and their environment. The collected information enables a wide

[1] Without loss of generality, we use the generic term *mobile participatory sensing* to designate applications using mobile phones as sensors (or as data sink for interfaced sensors) where participants contribute sensor data. The notion of participatory sensing therefore includes *mobiscopes* [1] and *opportunistic sensing* [2], spatial crowdsourcing [3], and mobile crowdsensing [4]. It also covers specific terminologies focusing on particular monitoring subjects, such as *urban sensing* [2], *participatory urbanism* [5], *citizen sensing* [6], *people-centric sensing* [1, 2], and *community sensing* [7].

range of innovative applications, ranging from people-centric to environmental-centric scenarios. With the help of people-centric applications, participants can monitor and document health-related issues, such as diet behaviors [8, 9, 10, 11], individual exposure and impact to air pollution [12, 13, 14, 15, 16], depression [17], physical activities [17, 18], sport experiences [19, 20, 21, 22, 23], and stress conditions [24]. Using the sensors embedded in their mobile phone, participants can also enhance social media [25, 26, 27] or contribute to price auditing applications [28, 29]. Additionally, they can contribute to monitor the mobility of crowds at large scale events, such as concerts or festivals [30, 31]. In contrast, environmental-centric applications crowdsource the collection of data about, e.g., urban air pollution [12, 5, 32, 33, 34, 35, 36], noise pollution [12, 37, 38, 39, 40, 41, 42, 43], weather conditions [44], events in the city [45], bus arrival times [46], or thermal columns [47].

Most of these applications have however been conceived as research prototypes and their real-world deployment still remains limited in terms of either number of participants or deployment duration as shown in Table 1. Nevertheless, comparable commercial products are increasingly gaining popularity among the population. For example, mobile applications, such as RunKeeper [48], Endomondo [49], and Nike+ Running [50] documenting running activities and MyFitnessPal [51] measuring calorie intakes totalize between 10 and 50 million installs only on the Google Play store. Connected bracelets, such as FitBit One [52], Jawbone Up [53], and Nike+ FuelBand [54], has represented a 330 million US dollars market in 2013 [55]. These statistics therefore confirm the existence and constant growth of the *Quantified Self* community [56, 57, 58, 59], which members rely on technology to better quantify, e.g., their fitness, performance, or sleep quality. Similarly, a commercial mobile micro-jobbing application called AppJobber [60] that relies on, e.g., pictures taken by participants counts over 100,000 registered users across different European countries that is more than most deployments compiled in Table 1. Consequently, mobile participatory sensing applications are not only limited to small-scale research prototypes, but are increasingly integrated in our daily life at a larger scale.

Table 1: Examples of real-world sensing deployments

Applications	Crowd size	Duration	Location
[14]	8 participants	1 month	La Jolla, USA
[15]	16 participants	2 to 4 weeks	La Jolla, USA
[30]	155 participants	8 days	Roskilde Music Festival, Denmark
[31]	128,000 participants	3 days	Züri Fäscht Festival, Switzerland
[43]	up to 13 participants	up to 1 week	Antwerp, Belgium
[45]	∼2,000 taxis	1 year	Stockholm, Sweden
[47]	2,331 participants	7 years	Switzerland

Both participants and end users can however put their privacy at risk when interacting with such applications. Since most collected sensor readings are annotated with spatiotemporal information, the participants' whereabouts can be inferred [61]. The sensor readings themselves may also reveal sensitive information about the contributing participants. Even end users who query application results may disclose their current location and potential interests. In order to address these threats, different countermeasures can be applied as shown in [61]. Building on our previous work, we herewith aim at reporting the latest progress in this area by especially analyzing newly proposed solutions. For this purpose, we adopt the same classification based on the different architectural components of typical participatory sensing applications. Consequently, this manuscript extends our previous survey and makes the following new contributions:

- We first analyze different scenarios in which the privacy of participants and end users may be endangered. As a result, we extend and refine our previous threat model, which primarily focuses on threats coming from administrators of participatory sensing campaigns.
- We next classify and examine how the current state-of-the-art in privacy-preserving solutions tackles the aforementioned threats. In this analysis, we especially consider recent approaches that have emerged in the last three years and are thus not covered in our previous work.
- Based on the surveyed solutions, we finally study the research challenges

which have been addressed and identify those which still need to be targeted in the future.

We present these contributions as follows. In Sec. 2, we recall the typical participatory sensing architecture. We next address privacy issues resulting from potential interactions with participatory sensing applications in Sec. 3, before detailing novel privacy-preserving solutions specially tailored for this scenario in Sec. 4. After examining past and current challenges in Sec. 5, we conclude this manuscript in Sec. 6.

2. Participatory Sensing Architecture

In what follows, we adopt the system model illustrated in Fig. 1, which serves as underlying basis for this manuscript. Participatory sensing applications include the participants' mobile phones and one or several application servers maintained by the campaign administrators. End users (i.e., the participants themselves or any other persons interested in the campaign) can leverage additional devices, such as laptops or desktop computers, to access the results of the participatory sensing campaign. The different stakeholders typically interact with the system components as follows:

1. *Tasking*: The campaign administrators or end users first determine the sensing tasks to be executed, which are then distributed to the participants' mobile phone.
2. *Sensing*: The participants' mobile phone collects the sensor readings corresponding to the defined sensing tasks.
3. *Local processing and storage*: The collected sensor readings may be locally processed on the mobile phone to, e.g., extract interesting features. The processed sensor readings may be temporarily stored by the participants before being transmitted to the application server.
4. *Reporting*: The participants' sensor readings are reported to the application server for further analysis and display.

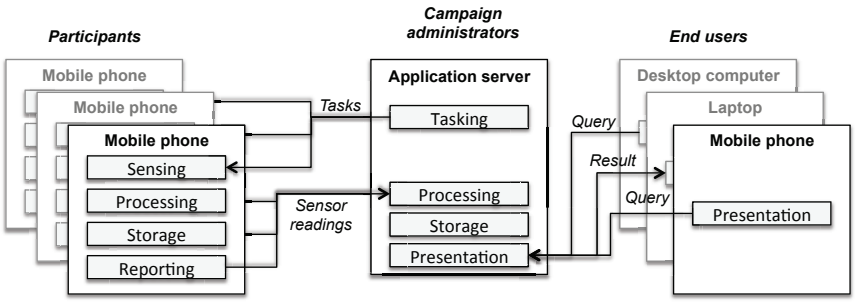

Figure 1: System overview

5. *Centralized storage and processing*: The application server may first store all reported sensor readings before analyzing them. It can then, e.g., remove incorrect sensor readings, compute summaries, or analyze the reported sensor readings.
6. *Presentation*: End users can access the results of the sensing tasks made available by the campaign administrators. For example, they can query specific sensor modalities or results in a region of interest.

3. Privacy Issues

Although participatory sensing systems undeniably provide novel opportunities in terms of sensing, they can put the privacy of the participants and end users at stake. For example, we have observed in our previous survey that most applications collect spatiotemporal information about the participants. This information is usually used to annotate the collected sensor measurements, such as sound samples, pictures, pollution and biometric data or the phones' acceleration. As a result, they can provide a wealth of insights about the participants, ranging from their current context to their behavior. We therefore highlight potential threats to privacy in Sec. 3.1. We next define a threat model in Sec. 3.2 summarizing possible privacy attacks conducted against the system described in Sec. 2.

3.1. Threats to Privacy

Participatory sensing campaigns first threaten the *participants*' privacy. In absence of any protection mechanisms, the participants' identity and location can be revealed when interacting with the system (e.g., when downloading the tasks from the application server or reporting sensor readings to the server). Assuming that the participants would use pseudonyms to contribute to participatory sensing applications, this would not efficiently protect their anonymity. Indeed, their identity (or at least a link between their different contribution) may still be inferred based on an analysis of the spatiotemporal annotations [62]. For example, a reverse look-up address search may reveal their name, as participants typically commute between their domicile and workplace. Alternatively, a cross-analysis of the participants' mobility patterns could enable their re-identification based on their uniqueness [63]. Such mobility patterns may also reveal participants' routines and habits, medical state based on frequent visits to hospitals and political affiliations [23].

Furthermore, the current participants' location may also be identified based on the collected sensor readings. For example, pictures, audio samples, and pollution data may include unique features, exposing the participants' whereabouts. When looking closer at the sensor readings, those can reveal fine-grained details about the participants. For example, accelerometer data can reveal the participants' current activities [64], their identity based on gait recognition [65], and their keyboard inputs, such as passwords [66, 67]. Additionally, participants can be re-identified based on the characteristics of the sensor readings they have collected [68].

Apart from the participants, *end users*' privacy can also be endangered. Assuming that end users can send query to the application server to retrieve sensor readings or subscribe to different data streams. By doing so, end users may provide knowledge to the campaign administrators about themselves. Their location can be first disclosed when sending a query, but also based on the query's content. In fact, it is likely that end users are interested in data collected

in their proximity. Similarly, queries and subscriptions can reveal insights about their personal interests.

3.2. Threat Model

In this section, we analyze different scenarios, in which the privacy of the participants and end users may be endangered. Note that this analysis extends the one conducted in [61], which primarily focuses on threats coming from the campaign administrators.

3.2.1. Internal Threats

We first consider possible threats coming from active stakeholders of participatory sensing applications, i.e., participants, campaign administrators, and end users. Theses threats can vary in terms of (1) degree of involvement, (2) sources and targets, (3) duration, and (4) background knowledge.

Concerning the *degree of involvement*, different scenarios are possible, ranging from involuntary to deliberate threats to others' privacy. For example, assuming that a participant reports her precise location to the application server, she can reveal the locations of other participants having reported coarser locations based on the similarities between the sensor measurements. In this case, the disclosure is not the result of a voluntary action conducted by this participant. On the opposite, campaign administrators could, e.g., actively collude with participants, who would report their precise locations on purpose to reveal those of other participants. Between both extrema, we can also imagine honest-but-curious stakeholders. Whereas they would behave normally (i.e., not conducting an active attack), they would be interesting in inferring information about others based on the data they have access to.

Among the different scenarios, both *sources* and *targets* can belong to either the same stakeholders' subset (i.e., participants, campaign administrators, or end users) or different ones. For example, participants may impersonate other participants and reveal sensitive data about them [69]. Alternatively, end users may attempt to deanonymize contributing participants based on the available

data. Moreover, the number of involved sources and targets may vary depending on the attack severity. Additionally, sources and targets can be either in physical proximity or randomly distributed [70, 71].

The *duration* of potential threats may also be different. For example, we can imagine continuous as well as time-limited attacks [70, 71]. Such attacks could be concentrated around particular times of interest, randomly distributed, or periodically programmed.

Malicious stakeholders may finally come with different *background knowledge* that they can combine with information available through the participatory sensing applications to ease their attacks or increase their severity [72]. For example, campaign administrators may use the registration information including their home address to re-identify participants using pseudonyms.

Note that we have previously focused on potential threats coming from participants, campaign administrators, and end users. We have deliberately not considered the network operator. The reason behind this exclusion is that the network operator needs to be trusted to respect the stakeholders' privacy, as it de facto has access to the unique phones' identifier and their locations [73, 74, 75].

3.2.2. External Threats

Like most existing systems, participatory sensing applications can also be subject to external attacks. In this case, an external attacker may attempt to gain insights about the participants and/or the end users. For example, they may be interested in knowing their identity, location, current context, or personal interests. To this end, they may hence attack (1) the application server to get access to the stored data or (2) he communication between the participants and/or the end users with the application server. Again, these threats are not specific to participatory sensing and well-established solutions can be applied to protect the concerned stakeholders from these threats.

In summary, threats to privacy resulting from participatory sensing applications can be diverse. While this list is by no means exhaustive, it aims at

increasing the awareness of future application developers and providing pointers for future privacy-preserving mechanisms.

4. Current State-of-the-Art

We herein present recently published privacy-preserving solutions that address the threats to privacy highlighted in Sec. 3.2. For this purpose, we build upon our previous work and classify novel solutions based on the architecture introduced in Sec. 2. For each studied solution, Tab. 2 summarizes the origin and target of the addressed threats to privacy.

4.1. Tasking

The starting point of all participatory sensing applications is the distribution of the tasks to the participants' mobile phone. While this first step may seem innocuous, it may already provide insights about the participants' identity, device, as well as current location when, e.g., downloading the tasks to be executed.

To prevent the campaign administrators from inferring this information, different solutions have already been proposed, such as using tasking beacons, attribute-based authentication, location privacy-preserving routing schemes [76], or downloading the tasks in densely populated locations [77]. In addition to these solutions, the novel *PiRi* scheme introduced in [78, 79] proposes to rely on the participants to distribute the tasks among them. To this end, each participant defines a region around her current location and merges it with the region of $k-1$ other participants to obtain a larger region. Instead of transmitting all computed regions, only elected participants transmit their extended region. The tasks distributed by the campaign administrators to these elected participants are then redistributed between all participants according to the region they are able to cover. By doing so, the campaign administrators do not gain access to the individual participants' location. Based on this approach, the same authors propose *TAPAS* [80], which aims at improving the quality of the

Table 2: Overview of the threats, sources, and targets addressed in the analyzed solutions as well as the corresponding applied techniques (*ID*: Identity, *L*: Location, *SR*: Sensor readings, *Pa*: Participants, *A*: Administrators, *EU*: End users, *B*: Bystanders, *Ps*: Pseudonyms, *k*: k-anonymity, *C*: Cryptography, and *D*: Differential privacy). x and (x) represent primary and secondary aspects, respectively.

Category	Solutions	Threats to			Threats from			Targeting			Techniques			
		ID	L	SR	Pa	A	EU	Pa	B	EU	Ps	k	C	D
Tasking	[76]	x	x			x		x					x	
	[77]	x	x			x		x					x	
	[78, 79]	x	x			x		x			x	x		
	[80]	x	x			x		x			x	x		
	[81]	x	x		(x)	x		x				x	x	
	[82]	x	x		(x)	x	x	x						x
	[83]	x	x		(x)	(x)	x	x				x		
Sensing	[85]	x	x			x	(x)	x			x	x		
	[86]	x	x				(x)		x					
Local storage	[87]		x	x		x		x					x	
Reporting	[77]	x	x			x	(x)	x				x	x	
	[88]	x				x	(x)	x						
	[89, 90]	x	x			x	(x)	x						
	[91]	(x)	(x)	x		x	(x)	x					x	
	[92]	x	(x)	x		x	(x)	x				x	x	
	[93]		x			x	(x)	x				x		
	[94]	x	x			x	(x)	x			x	x		
	[95]		x			x	(x)	x				x		
	[96]	(x)	x			x	(x)	x				x		
	[97]	x				x	(x)	x			x			
	[98, 99]	x				x		x			x	x	x	
	[100]	x				x		x			x	x		
	[101]	x				x		x			x		x	
	[102]	x				x		x			x		x	
	[103]	x				x		x			x		x	
	[104, 105]	x				x		x			x		x	
	[106]	x				x		x			x		x	
	[107]		(x)	x		x	(x)	x					x	
	[108]		x			x	(x)	x					x	
	[109]		x			x		x			x		x	
	[110]	x	x			x	(x)	x				x	x	
	[111]		x	x	x	x		x						
	[112]		x			x		x						
	[113]		x	x		x		x						
	[114, 115]		x	x	(x)	x		x				x	x	
	[116]		(x)	x	(x)	x		x					x	(x)
	[117]		(x)	x	(x)	x		x					x	x
	[118]		(x)	x	(x)	x		x			x		x	
	[119]		x			x		x						
Storage & access control	[120, 121]		x	x			x	x						
	[122, 123]													
	[124]		x				x	x						
Presentation	[125]		x			x	x	x					x	
	[70, 71]	x	x			x	x	x					x	
	[126]	x	x			x				x			x	
	[73, 74]	x	x			x		x		x	x		x	
	[75]													

collected sensor readings by optimizing the participants' selection in proximity of a particular location of interest while still protecting their location privacy. In both cases, the privacy protection however fully depends on the participants' trustworthiness and can hence be endangered as soon as the participants would, e.g., collude with the campaign administrators.

An alternative to *PiRi* and *TAPAS* is to use a central trusted entity to build the cloaked region based on the k nearest participants to a point of interest as proposed in [81]. In this case, the participants however provide their location to the trusted entity. They therefore need to trust this entity to efficiently protect their data against external attacks and also not to disclose it to unauthorized entities.

As a result, participants can cloak their location using either distributed or centralized mechanisms based on other participants or a trusted entity, respectively. In both cases, the task distribution between participants using cloaked locations can be optimized. For example, the solution proposed in [127] aims at increasing the task fulfillment rate while simultaneously minimizing the distance to cover by the participants to fulfill these tasks.

Instead of relying on either other participants or a trusted entity, the network provider plays the role of a broker between the participants and the application server in [82]. The participants first transmit their location to the network provider. Note that involving the network provider in this scheme does not increase the risks for the participants' privacy, as it already knows the participants' location. The application server can then query the network provider to find participants willing to fulfill tasks in a region of interest. Instead of providing the identity and location of potential participants, the network provider adds random noise to the query results based on the concept of differential privacy [128]. As a result, the application server cannot infer whether a particular participant is located in a particular region based on its queries. Finally, the application server uses the answer of the network provider to contact potential participants using geocasting. If the contacted participants are willing to contribute to the task, they answer back to the application server, which hence

infers their identity. Otherwise, they remain silent and thus unknown from the application server. Consequently, the network provider simultaneously protects the participants' location privacy by leveraging differential privacy, while allowing the application server to distribute sensing tasks to voluntary participants based on their location. Following the same idea of privacy brokers, the approach proposed in [83] enables end users to directly distribute tasks to the participants. In this case, mobile cloud agents are responsible for managing the distribution of the tasks in a decentralized fashion. Again, the participants need to trust them to respect and apply their privacy preferences.

4.2. Sensing

Assuming that the sensing tasks have been distributed to the participants' mobile phone. Participants' may then be able to control *ex ante* the degree of granularity at which the sensor readings are collected depending on their individual privacy preferences. As enabler for this control, we have proposed different interfaces allowing participants to choose between three degrees of granularity for the collection of location information, sound samples, pictures and acceleration data [84]. We have further introduced picture-based warnings based on the participants' current privacy settings in [129]. These warnings aim at increasing the participants' awareness about potential risks for their privacy and allow them to then accordingly adapt their settings if necessary. Note that both approaches can also be applied *post ante* before sharing the collected data with the application server without loss of generality.

Additionally, the participants can define zones in which no sensor readings are either collected or reported to the application server. Setting such zones may however not be sufficient to efficiently protect the participants' privacy. For example, they may only contain the participant's home and hence indirectly reveal her identity. In order to prevent this issue, the solution proposed in [85] includes an underlying mechanism that automatically adapts the zone to cover at least k buildings. As a result, the so called *silent zones* dynamically optimize

the existing tradeoff between privacy protection and data granularity based on the density of surrounding buildings.

4.3. Local Processing and Storage

After the collection of the sensor readings, local processing can be applied on the participants' phones to remove privacy-sensitive features. For example, sound samples including human voices may be discarded. After processing, the remaining sensor readings may then be stored on either the participants' mobile phones or individual repositories. For example, participants can securely store their collected on cloud servers using the approach introduced in [87]. By encrypting them using proxy re-encryption and homomorphic encryption, the sensor readings are not accessible by untrusted cloud providers, but can be accessed by participatory campaigns selected by the participants.

4.4. Data Reporting

When reporting sensor readings to the application server, the following techniques can be applied to protect the participants' privacy.

4.4.1. Anonymity

To ensure the participants' anonymity, several solutions leverage the concept of mix networks [130] or mix zones [131]. The key idea is that the participants' contributions are mixed with others when sent to the application server to prevent the campaign administrators from identifying their original source. Multiple servers ensure this function in [77] by mixing different contributions, rerouting them, and introducing delays. In [88], the participants themselves serve as routers and a multi-hop route is built between the participants, along which each participant only knows her predecessor and successor. When the sensor readings reach the tenth participant, they are uploaded to the application server. This scheme however requires maintaining a peer-to-peer network between the participants and coping with, e.g., disconnections.

An alternative is to leverage opportunistic encounters between participants to exchange collected sensor readings when being in physical proximity [89, 90].

This scheme called *path jumbling* however fully depends on the participants' trustworthiness and collaboration. To quantify the trust level of the participants and quarantine untrustworthy ones, *TrustMeter* approach has therefore been introduced in [132]. Participants can leverage it associated with dedicated user interfaces detailed in [133] to set the minimum trust level required by other participants to be able to exchange sensor readings with them. Moreover, the participants can select different exchange strategies between exchanging: (1) all sensor readings, (2) a random number of sensor readings, or (3) a number of sensor readings agreed between both exchange partners. Instead of exchanging full or partial sets of sensor readings, *SLICER* [92] inspired by [91] proposes to either exchange only one sensor reading at each encounter or select a subset of participants to share more sensor readings with and hence optimize the reporting process.

Instead of considering individual sensor readings, the following mechanisms focus on the participants' full trajectories. By using [93, 94], the participants can conceal their own trajectories with those of other participants based on a trusted third party. In [93], the trusted third party merges the sensor readings belonging to different participants to build new equivalent trajectories. Alternatively, the trusted third party maps the identities and the participants' trajectories entering and leaving predefined sensitive zones in *TrPF* [94]. By doing so, the mixing function can be customized and optimized depending on the desired privacy protection. While this control can be an advantage as compared to the concept of physical mixes, the solution however requires that the participants provide their precise location to this third party.

To prevent the third party from linking the participants' identity to their location, the participants first collaborate by relaying the other participants' sensor readings before uploading them to the third party in [95]. The third party then anonymizes the sensor readings and sends them back to the participants following the same route. Since the sensor readings have been previously anonymized, the participants can report them to the application server using their real identity. Note that the number of participants is however unlimited

as compared to [88].

Such centralized architectures however present a single point of failure, making them vulnerable to malfunctions and external attacks. *LOCATE* [96] therefore adopts a distributed approach by leveraging a direct collaboration between the participants. In this case, not a third party needs to be trusted, but other participants. To mitigate this trust in other participants, two sets of the original participants' trajectories are built. Assuming that a user frequently visited n locations. The first set consists of trajectories including $n' < n$ of the frequently visited locations. In the second set, none trajectory contains any of the n locations. The number of trajectories belonging to each set is computed based on the resulting entropy. The participants alternatively exchange trajectories from both sets and distribute the exchanges over time between different participants.

4.4.2. Pseudonymity

To protect the participants' privacy, various applications replace the participants' real identity by a unique pseudonym, including [134, 29, 23, 97]. However, it has already been shown in [62] that the provided protection is insufficient, as the real identifies may be inferred based on the reported location information. In [97], the participants have the possibility to mitigate this threat by dropping the collected sensor readings, if they estimate that they could endanger their anonymity. This however requires a manual intervention of the participants before each reporting. Moreover, it is assumed that the participants can correctly identify privacy threats by, e.g., taking into account their past contributions, which may not always be the case.

An alternative to unique pseudonyms is proposed in the *IncogniSense* framework [98, 99], which relies on the utilization of periodic pseudonyms and a transfer of reputation between these pseudonyms. By doing so, the framework combines to conflicting aspects namely the participants' privacy and reputation. Indeed, most reputation and incentive schemes require a link between the participants' contributions over time to, e.g., identify participants contributing incorrect measurements or reward active participants. In contrast, protecting the

participants' privacy often requires to break the link between the participants' contributions. Moreover, the chosen approach is independent of any trusted third parties because of the utilization of blind signatures. If blind signatures theoretically ensure that successive pseudonyms cannot be linked, the evolution of the pseudonyms' reputation may reveal their chronology. To prevent such linking attacks, the reputation transferred between pseudonyms is cloaked to build groups sharing similar reputation values and render the pseudonyms indistinguishable.

Building upon periodic pseudonyms, different alternatives have been introduced. For example, a trusted third party is responsible for building the pseudonyms' groups [100]. In comparison to IncogniSense, this approach enables a dynamic adaptation of the cloaked values, but the trusted third party knows the link between the participants' identity and their pseudonyms in addition to their original and cloaked reputations values. Another alternative also based on blind signatures or a trusted third party adds an incentive mechanism on top of the reputation framework to reward contributing participants [101]. The idea of rewarding participants using pseudonyms is shared with [102] and [103]. In the former approach, participants use a unique pseudonym, while they use multiple pseudonyms in combination with a group signature scheme in the latter called *SPPEAR*. Instead of only supporting positive reputation updates as in the aforementioned approaches, the solution called *ARTSense* proposed in [104, 105] also allows negative reputation updates. This aims at further penalizing malicious participants by increasing the impact of incorrect measurements on their reputation. When adopting the *LotS* framework [106], the identity of misbehaving participants may even be revealed.

4.4.3. Spatial Cloaking

As we have seen in Sec. 4.4.1 and 4.4.2, the above solutions protect the participants' privacy by breaking the link between their identity and contributions. By mixing the contributions between participants or utilizing different pseudonyms, most presented solutions preserve the original spatiotemporal in-

formation. Other methods alter the location information by providing it at a coarser degree of granularity and/or building groups of k participants sharing the same location. Note that a comparison of both methods [72] shows that the degree of granularity has additional influence on the participants' location privacy than the number of participants sharing the same location.

Instead of selecting a predefined degree of granularity before the measurements (cf. Sec. 4.2), dynamic solutions, such as *ipShield* [107] and that presented in [108], can be applied. These solutions running on the participants' mobile phone consider the participants' current context and past contributions to compute the appropriate degree of granularity at which the location information can be released to the application server. As a result, end users will have access to this data with either the same (if the campaign administrators release the data as such) or a coarser degree of granularity (if the campaign administrators apply further processing).

However, providing both coarse-grained information to the application server and fine-grained information to specific end users can be useful in certain application scenarios. For example, participants may be willing to share detailed information, such as the time of their asthma crisis, with their doctor to analyze its potential environmental causes but not with other end users. This is possible with the scheme proposed in [109]. It releases the location information at two different degrees of granularity: the coarsest one is anonymized and publicly available, whereas the finest one is encrypted using attribute based encryption. This means that only end users showing the attributes defined by the participants (e.g., age, location, role...) will be able to decrypt and have access to the participants' fine-granular locations.

Instead of adapting the degree of granularity to potential data recipients, the approach introduced in [110] applies two different techniques based on the size of the area of interest, which is assumed to be centered on a predefined point of interest. In the case of large areas, the participants replace their precise location by the nearest point of interest and report the corresponding sensor readings to a broker. The broker aggregates them and transmits the results to

the application server. By applying this technique, the location granularity is hence degraded. In contrast, the participants apply double encryption on the sensor readings including their precise location in the case of small areas. They use first the application server's public key, before using the broker's public key. Again, the encrypted sensor readings are sent to the broker, which waits for several participants to do the same before forwarding them to the application server. By doing so, the location granularity is preserved but the link between the participants' identity and contributions is broken by the intermediary of the broker. Therefore, this hybrid approach dynamically leverages the concepts of either spatial cloaking or aggregation (cf. Sec. 4.4.5) depending on the size of the monitored area.

4.4.4. Data Perturbation

The key principle of data perturbation is to hide the individual participants' contributions while allowing the application server to computes statistical trends over the whole participants' set. To hide the individual contributions, the first method consists in adding noise on the participants' sensor readings. As a result, the noise selection determines the participants' privacy protection.

Assuming that all participants share the same noise distribution. There is a risk that malicious participants may be able to reconstruct it based on their own data and hence breach the privacy of other participants. To mitigate this threat, the authors propose the *PESP* scheme [111], which distributes different noise distributions to the participants and adapt them to the sensor readings already reported to the application server.

Instead of automatically adapting the individual noise distributions, *ALPS* [112] adjusts the perturbation according to the participants' preferences. As a result, a tailored Gaussian perturbation is first applied followed by a smoothing function to remove potentially remaining insights about the participants and hence protect their privacy.

An alternative to using noise is to leverage the concept of negative surveys as introduced in [113]. In this case, the collected sensor readings are divided

into different complementary categories. Instead of reporting their own sensor readings, the participants choose sensor readings from another category and report those to the application server. Using a perturbation matrix that maps the probability of perturbing a category to another, the application server is able to reconstruct the probability density functions of the original sensor readings without having access to them.

4.4.5. Data Aggregation

The idea behind data aggregation is also to break the link between the participants' identity and their contribution. In contrast to the mechanisms detailed in Sec 4.4.1, sensor readings from different participants are however merged together to build aggregates. The application server receiving the aggregates is hence unable to isolate individual sensor readings and link them to the collecting participants. Different methods can be applied to aggregate the data, ranging from centralized to distributed solutions. For example, *NoiseTubePrime* [114, 115] relies on a network of trusted brokers. The participants report their results on a map common to all participants and encrypted using the campaign administrators' public key to their respective broker. The brokers organized in a ring topology successively add the contribution of their participant until the aggregate map is completed.

By applying the scheme proposed in [116], participants however not need to trust one or several aggregators (such as the brokers in NoiseTubePrime). The authors make use of additive homomorphic encryption combined with a new key management scheme to reduce both the communication and encryption overhead while still supporting sum and min aggregates. To better support the participants' dynamic (i.e., new participants joining or leaving), the original scheme has been extended in [117] by a novel ring-based interleaved grouping technique that diminishes the number of participants that need to renew their cryptographic keys.

Also not trusting the aggregator, *VPA+* [118] adopts a hybrid solution, in which the participants first register their sensor readings to the aggregator

before contributing them to the aggregate computed in a distributed fashion. Using a homomorphic MAC of the participants' sensor readings, the registration does however not reveal the original data but allows the aggregator to later verify which participants have contributed and hence guarantee the aggregate's integrity. Similarly, the participants collaborate to compute the sum aggregate without revealing the individual sensor readings.

4.5. Hiding Selective Locations

The solution proposed in [119] is devised for application scenarios, in which the temporal annotations of the sensor readings are irrelevant. In such cases, the participants explicitly choose the sensor readings corresponding to the locations they want to share with the application server. Their mobile phone then mixes them to modify their chronology and hence break the link between both spatial and temporal information. As a result, the application server can compute the application results based on the data voluntarily shared by the participants.

4.6. Storage and Access Control

The sensor readings reported to the application server can be either individually stored or directly processed on the application server to build, e.g., statistics or maps. The participants may thus only maintain control over their data in the former case. For this purpose, they may use dedicated access control and data sharing solutions, such as *SensorSafe* [120, 121, 122, 123] or *PDVLoc* [124]. Using SensorSafe, the participants can manage several individual repositories using a broker and tailor the granularity at which the collected data are shared based on, e.g., its nature and context, the resolution required by potential end users, their identity or attributes, as well as the degree of trust of the participants in these end users. Following a similar model, PDVLoc allows participants to select potential data recipients as well as the corresponding degree of granularity at which the data is shared. It further supports the participants in configuring their settings and shows them the consequences of their decisions. An additional function notifies the participants when their current settings seem to diverge from their personal conception.

4.7. Presentation

Participatory sensing results can be made available to end users in different forms. For example, end users may access a map aggregating all participants' results or be able to query and filter individual results based on, e.g., a region, sensor modality, or operating system of interest. As soon as end users are able to query participatory sensing results, the privacy of both participants and end users may be put at stake.

Among the existing solutions, the one proposed in [125] concentrates on protecting the participants' privacy. For this purpose, the participants report only partial trajectories to the application server, which then optimizes the query answers by merging partial data collected by several participants. Instead of submitting only partial results, the participants encrypt their complete sensor readings and distribute multiple duplicates to other participants at regular and common time intervals in [70, 71]. The encrypted sensor readings are annotated with a tag corresponding to the time interval at which they have been collected and exchanged. End users can then send a query indicating the sensor readings and interval of interest to a gateway, which will forward it to a set of participants. Participants matching the query provide the corresponding encrypted sensor readings to the end users through the gateway. As a result, neither the gateway nor the end users can infer who has initially collected the sensor readings, as the link between the participants' identity and their contribution are broken during the exchanges.

Besides, *PEPPeR* [126] only focuses on end users' privacy and relies on tokens distributed by the application server to authorized end users. By using them, end users can directly query participants, who provide access to their sensor readings once they have verified the corresponding token with the application server. The verification process however does not disclose the identity of the end users to the application server and preserves hence their privacy.

In comparison, *PEPSI* [73, 74, 75] simultaneously protects the privacy of both participants and end users. It relies on a trusted third party responsible for their registration and authorization. During the campaign, the registered par-

ticipants report their sensor readings encrypted to the application server, while the registered end users send their queries to the application server. Leveraging authorizations and tokens delivered by the trusted third party during the registration process, the application server blindly matches both sensor readings and queries. This means that both collected data and query content remain hidden from the application server.

5. Past and Future Challenges

We have highlighted the progress of privacy-preserving schemes for participatory sensing applications in the past years. While this domain still attracts many novel solutions, some privacy challenges still remain. In what follows, we successively consider the research challenges identified in our previous survey and discuss how these have been addressed, before highlighting novel research directions.

5.1. Including Participants in the Privacy Equation

Among the previously identified challenges, this is probably the one which has been the most addressed in the last years. The participants were initially only able to choose the granularity at which sensor readings are collected, manage individual storages, and control the data stored and disclosed to end users. We now observe an increasing inclusion of the participants in the control of novel privacy-preserving mechanisms. For example, their privacy preferences is taken into account during both the tasking and the reporting processes (see Sec. 4.1 and Sec. 4.4, respectively). To cater for this control, specific interfaces have been designed and evaluated based on user studies. In addition to server in the evaluation of technical approaches, user studies, such as [135] and [136], have been conducted to analyze potential users' privacy expectations and how these are influenced by contextual factors (e.g., sensing modality, duration, or purpose of the data collection). While the first stones have recently been laid, additional efforts are needed to cater for additional privacy control and

awareness. This however remains challenging as it requires to finely balance the trade-off between control and the resulting overhead for the participants. Moreover, finding representative and large user sets makes the evaluation of future approaches demanding.

5.2. Providing Composable Privacy Solutions

All aforementioned approaches still focus on providing a particular mechanism to address one specific threat to privacy at a time. This means that none of them addresses the full spectrum of possible threats to privacy. Application developers still need to select each mechanism individually. Instead, an integrated holistic solution is required to help them in selecting appropriate mechanisms depending on the specifications of their application. Besides, this solution should be easily and intuitively configurable.

5.3. Trade-offs between Privacy, Performance, and Data Fidelity

An increasing number of mechanisms consider potential trade-offs linked to the respect of the privacy of the participants and end users. For example, solutions have been proposed to (1) optimize the sensing coverage during the task distribution process (cf. Sec. 4.1), (2) optimize the incentives given to the participants depending on the expected quality of information [137], and (3) run reputation algorithms (cf. Sec. 4.4.2). All of them simultaneously respect the participants' privacy. Pursuing in this direction is necessary as both application utility and participants' privacy are two tightly-coupled key components in the acceptance of both participants and end users. If the application utility is limited, end users may not be interested in the results. The same is valid for the participants: if their privacy is not respected, they may not be willing to contribute to the application and hence limit its utility.

5.4. Making Privacy Measurable

Most solutions are evaluated using different privacy metrics. Depending on the scenario, the authors either introduce a new metric or choose an existing

one. Existing metrics include k-anonymity, l-diversity, entropy-based, errors-based, or probabilistic-based [138]. As before, this makes a comparison of the performance of the different schemes difficult. However, more and more solutions adopt a decentralized or distributed setting. By doing so, they reduce the trust that the participants need to have in a unique entity to guarantee the protection of their privacy.

5.5. Defining Standards for Privacy Research

While some studied approaches share the same dataset for their evaluation, there is still no consensus on a common open data set, which would be adopted by all to ease the comparison of the proposed schemes. As compared to other research fields, only few schemes are thoroughly compared against each other especially in terms of performance using, e.g., simulations. Not having a benchmarking corpus in terms of dataset and open privacy solutions hence prevent application developers from easily identifying and selecting the best solution to address privacy threats.

5.6. Holistic Architecture Blueprints

In comparison to our previous survey, we have observed an increased diversity among the sources and targets of privacy threats addressed in the studied approaches. Instead of only focusing on threats coming from the campaign administrators and targeting the participants, recent solutions highlighted in Tab. 2 address the privacy protection of both participants and end users. This fact might be linked with the evolution of the underlying participatory sensing applications. In the first proposed applications, end users are mostly only able to access already collected information displayed, e.g., in forms of maps or statistics. In contrast, end users can also trigger the collection of sensor readings depending on their own interests in recently developed applications. Having this capability, end users have hence recently moved from a passive to a more active role in the system. Such evolution leads to an increase of the threats to their privacy. Tailored privacy-preserving mechanisms to these specific threats

are therefore needed. However, only few solutions address threats coming or targeting different groups of stakeholders. While the existing solutions can still be composed to provide a complete solution, it may be useful for application developers to have a solution covering most to all threats to privacy.

In summary, most of the challenges identified in our previous survey have still not been fully tackled and require additional attention. The following challenges complete our list of previously identified challenges based on the solutions surveyed in this manuscript.

5.6.1. Bystander Privacy

Most of the studied schemes consider each participant as an individual entity and omit their relationships with others (i.e., participants or non-participants). By doing so, this poses the risks for participants to unwillingly reveal information about others. For example, collected sound samples can reveal private conversations of bystanders or similar sensor readings can disclose the proximity of two or more participants as shown in [68]. To prevent this scenario, the participants can leverage *NotiSense* [86], which notifies the participants about currently running sensing tasks and potential risks for their privacy. While this approach offers a first solution to this issue, we believe that additional alternatives can be devised by, e.g., integrating this aspect in the privacy-preserving solutions to be developed.

5.6.2. Multidimensional Privacy

The aforementioned approaches mainly focus on the annotation of the collected sensor readings. Different solutions are proposed to hide, cloak, perturb, or aggregate them. Only little attention is however given to the collected sensor readings themselves. While the collection of sensor readings is the key characteristic of participatory sensing and solutions tailored to this scenario might hence only be transferable to other research domains to a limited extend, the sensor readings can also endanger the participants' privacy as highlighted in Sec. 3.1. Additional emphasis should therefore be put on the sensor readings themselves

and more especially, on the impact of their combination and correlation on the participants' privacy.

5.6.3. Internet of Things and Smart Cities

Up to now, the developed mechanisms have been tailored to participatory sensing and only consider data collected using the participants' mobile phones. However, participatory sensing may not evolve to a stand-alone paradigm. In the future, it may be integrated into the vision of the *Internet of Things*, where all participants' devices and appliances are foreseen to be connected and collaborate to fulfill different tasks. In this scenario, the sensor readings collected by the mobile phones might complete the information provided by other devices. By extending the scale of this vision, mobile phones can also be part of the next concept of *Smart Cities*. Again, bystander privacy (or "passive sensing") plays a major role here because building owners can collect data about people without their consent. Their integration will however pose new privacy threats and solutions to cover the collection of multidimensional information about the citizens are still to be designed.

6. Conclusions

We have reported on the latest trends in the area of privacy in participatory sensing. For this purpose, we have classified and analyzed recently proposed privacy-preserving approaches. Based on this analysis, we have refined the threat model that apply in this field and studied how solutions recently emerged address the research challenges identified in [61]. While some challenges have been tackled, there is a strong need to future research, especially when considering the integration of participatory sensing in larger visions, such as the Internet of Things or Smart Cities. By introducing more and more information about the physical world into the digital space, the privacy of the citizens' will be increasingly endangered and novel approaches tailored to such scenarios are needed.

Acknowledgment

The author would like to thank A. Reinhardt as well as the anonymous reviewers for their valuable comments and suggestions.

References

[1] T. F. Abdelzaher, Y. Anokwa, P. Boda, J. A. Burke, D. Estrin, L. Guibas, A. Kansal, S. Madden, J. Reich, Mobiscopes for Human Spaces, IEEE Pervasive Computing 6 (2) (2007) 20–29.

[2] A. T. Campbell, S. B. Eisenman, N. D. Lane, E. Miluzzo, R. A. Peterson, H. Lu, X. Zheng, M. Musolesi, K. Fodor, G.-S. Ahn, The Rise of People-centric Sensing, IEEE Internet Computing 12 (4) (2008) 12–21.

[3] L. Kazemi, C. Shahabi, GeoCrowd: Enabling Query Answering with Spatial Crowdsourcing, in: Proceedings of the 20th International Conference on Advances in Geographic Information Systems (SIGSPATIAL), 2012, pp. 189–198.

[4] R. K. Ganti, F. Ye, H. Lei, Mobile Crowdsensing: Current State and Future Challenges, IEEE Communications Magazine 49 (11) (2011) 32–39.

[5] E. Paulos, R. Honicky, E. Goodman, Sensing Atmosphere, in: Proceedings of the Workshop on Sensing on Everyday Mobile Phones in Support of Participatory Research (SenSys Workshop), 2007, pp. 15–16.

[6] J. A. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, M. B. Srivastava, Participatory Sensing, in: Proceedings of the 1st Workshop on World-Sensor-Web (WSW), 2006, pp. 1–5.

[7] A. Krause, E. Horvitz, A. Kansal, F. Zhao, Toward Community Sensing, in: Proceedings of the 7th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN), 2008, pp. 481–492.

[8] S. Reddy, A. Parker, J. Hyman, J. A. Burke, D. Estrin, M. Hansen, Image Browsing, Processing, and Clustering for Participatory Sensing: Lessons from a DietSense Prototype, in: Proceedings of the 4th Workshop on Embedded Networked Sensors (EmNets), 2007, pp. 13–17.

[9] M. Annavaram, N. Medvidovic, U. Mitra, S. Narayanan, G. Sukhatme, Z. Meng, S. Qiu, R. Kumar, G. Thatte, D. Spruijt-Metz, Multimodal Sensing for Pediatric Obesity Applications, in: Proceedings of International Workshop on Urban, Community, and Social Applications of Networked Sensing Systems (UrbanSense), 2008, pp. 21–25.

[10] T. Denning, A. Andrew, R. Chaudhri, C. Hartung, J. Lester, G. Borriello, G. Duncan, BALANCE: Towards a Usable Pervasive Wellness Application with Accurate Activity Inference, in: Proceedings of the 10th Workshop on Mobile Computing Systems and Applications (HotMobile), 2009, pp. 5:1–5:6.

[11] L. Nachman, A. Baxi, S. Bhattacharya, V. Darera, P. Deshpande, N. Kodalapura, V. Mageshkumar, S. Rath, J. Shahabdeen, R. Acharya, Jog Falls: A Pervasive Healthcare Platform for Diabetes Management, Pervasive Computing 6030 (1) (2010) 94–111.

[12] E. Kanjo, J. Bacon, D. Roberts, P. Landshoff, MobSens: Making Smart Phones Smarter, IEEE Pervasive Computing 8 (4) (2009) 50–57.

[13] M. Mun, S. Reddy, K. Shilton, N. Yau, J. A. Burke, D. Estrin, M. Hansen, E. Howard, R. West, P. Boda, PEIR, the Personal Environmental Impact Report, as a Platform for Participatory Sensing Systems Research, in: Proceedings of the 7th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys), 2009, pp. 55–68.

[14] E. Bales, N. Nikzad, N. Quick, C. Ziftci, K. Patrick, W. Griswold, Citisense: Mobile Air Quality Sensing for Individuals and Communities Design and Deployment of the Citisense Mobile Air-Quality System, in:

Proceedings of the 6th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth), 2012, pp. 155–158.

[15] P. Zappi, E. Bales, J. H. Park, W. Griswold, T. Š. Rosing, The Citisense Air Quality Monitoring Mobile Sensor Node, in: Proceedings of the 11th ACM/IEEE Conference on Information Processing in Sensor Networks (IPSN), 2012, pp. 1–5.

[16] B. Predic, Z. Yan, J. Eberle, D. Stojanovic, K. Aberer, ExposureSense: Integrating Daily Activities with Air Quality using Mobile Participatory Sensing, in: Proceedings of the 11th IEEE International Conference on Pervasive Computing and Communications (PERCOM Workshops), 2013, pp. 303–305.

[17] E. P. Stuntebeck, J. S. Davis, II, G. D. Abowd, M. Blount, HealthSense: Classification of Health-related Sensor Data through User-assisted Machine Learning, in: Proceedings of the 9th Workshop on Mobile Computing Systems and Applications (HotMobile), 2008, pp. 1–5.

[18] J. Hicks, N. Ramanathan, D. Kim, M. Monibi, J. Selsky, M. Hansen, D. Estrin, AndWellness: An Open Mobile System for Activity and Experience Sampling, in: Proceedings of the 1st Wireless Health Scientific Conference (WH), 2010, pp. 34–43.

[19] S. B. Eisenman, N. D. Lane, E. Miluzzo, R. A. Peterson, G. Ahn, A. T. Campbell, MetroSense Project: People-centric Sensing at Scale, in: Proceedings of the 1st Workshop on World-Sensor-Web (WSW), 2006, pp. 6–11.

[20] S. B. Eisenman, A. T. Campbell, SkiScape Sensing, in: Proceedings of the 4th ACM International Conference on Embedded Networked Sensor Systems (SenSys), 2006, pp. 401–402.

[21] S. B. Eisenman, E. Miluzzo, N. D. Lane, R. A. Peterson, G.-S. Ahn, A. T. Campbell, The BikeNet Mobile Sensing System for Cyclist Experience

Mapping, in: Proceedings of the 5th ACM International Conference on Embedded Networked Sensor Systems (SenSys), 2007, pp. 87–101.

[22] S. B. Eisenman, E. Miluzzo, N. D. Lane, R. A. Peterson, G.-S. Ahn, A. T. Campbell, BikeNet: A Mobile Sensing System for Cyclist Experience Mapping, ACM Transactions on Sensor Networks 6 (1) (2009) 1–39.

[23] K. Shilton, Four Billion Little Brothers?: Privacy, Mobile Phones, and Ubiquitous Data Collection, Communications of the ACM 52 (11) (2009) 48–53.

[24] H. Lu, D. Frauendorfer, M. Rabbi, M. S. Mast, G. T. Chittaranjan, A. T. Campbell, D. Gatica-Perez, T. Choudhury, StressSense: Detecting Stress in Unconstrained Acoustic Environments Using Smartphones, in: Proceedings of the 14th ACM International Conference on Ubiquitous Computing (UbiComp), 2012, pp. 351–360.

[25] S. Gaonkar, J. Li, R. R. Choudhury, L. Cox, A. Schmidt, Micro-Blog: Sharing and Querying Content through Mobile Phones and Social Participation, in: Proceedings of the 6th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys), 2008, pp. 174–186.

[26] E. Miluzzo, N. D. Lane, K. Fodor, R. A. Peterson, H. Lu, M. Musolesi, S. B. Eisenman, X. Zheng, A. T. Campbell, Sensing meets Mobile Social Networks: The Design, Implementation and Evaluation of the CenceMe Application, in: Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems (SenSys), 2008, pp. 337–350.

[27] M. Musolesi, E. Miluzzo, N. D. Lane, S. B. Eisenman, T. Choudhury, A. T. Campbell, The Second Life of a Sensor: Integrating Real-world Experience in Virtual Worlds using Mobile Phones, in: Proceedings of the 5th Workshop on Embedded Networked Sensors (HotEmNets), 2008, pp. 1–5.

[28] Y. Dong, S. S. Kanhere, C. Chou, N. Bulusu, Automatic Collection of Fuel Prices from a Network of Mobile Cameras, in: Proceedings of the 4th IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS), 2008, pp. 140–156.

[29] L. Deng, L. Cox, LiveCompare: Grocery Bargain Hunting through Participatory Sensing, in: Proceedings of the 10th Workshop on Mobile Computing Systems and Applications (HotMobile), 2009, pp. 1–6.

[30] A. Stopczynski, J. Larsen, S. Lehmann, L. Dynowski, M. Fuentes, Participatory Bluetooth Sensing: A method for Acquiring Spatio-temporal Data about Participant Mobility and Interactions at Large Scale Events, in: Proceedings of the 11th IEEE International Conference on Pervasive Computing and Communications (PERCOM Workshops), 2013, pp. 242–247.

[31] U. Blanke, G. Troster, T. Franke, P. Lukowicz, Capturing Crowd Dynamics at Large Scale Events using Participatory GPS-localization, in: Proceedings of the 9th IEEE International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2014, pp. 1–7.

[32] D. Mendez, A. Perez, M. Labrador, J. Marron, P-Sense: A Participatory Sensing System for Air Pollution Monitoring and Control, in: Proceedings of the 9th IEEE International Conference on Pervasive Computing and Communications (PERCOM Workshops), 2011, pp. 344–347.

[33] D. Hasenfratz, O. Saukh, S. Sturzenegger, L. Thiele, Participatory Air Pollution Monitoring Using Smartphones, Mobile Sensing (2012) 1–5.

[34] S. Devarakonda, P. Sevusu, H. Liu, R. Liu, L. Iftode, B. Nath, Real-time Air Quality Monitoring through Mobile Sensing in Metropolitan Areas, in: Proceedings of the 2nd ACM SIGKDD International Workshop on Urban Computing, 2013, pp. 1–15.

[35] K. Hu, Y. Wang, A. Rahman, V. Sivaraman, Personalising Pollution Exposure Estimates using Wearable Activity Sensors, in: Proceedings of the IEEE 9th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2014, pp. 1–6.

[36] W. Sun, Q. Li, C.-K. Tham, Wireless Deployed and Participatory Sensing System for Environmental Monitoring, in: Proceedings of the 11th IEEE International Conference on Sensing, Communication, and Networking (SECON), 2014, pp. 158–160.

[37] M. Bilandzic, M. Banholzer, D. Peev, V. Georgiev, F. Balagtas-Fernandez, A. De Luca, Laermometer: A Mobile Noise Mapping Application, in: Proceedings of the 5th ACM Nordic Conference on Human-Computer Interaction (NordiCHI), 2008, pp. 415–418.

[38] P. Mohan, V. Padmanabhan, R. Ramjee, Nericell: Rich Monitoring of Road and Traffic Conditions using Mobile Smartphones, in: Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems (SenSys), 2008, pp. 323–336.

[39] N. Maisonneuve, M. Stevens, M. E. Niessen, L. Steels, NoiseTube: Measuring and Mapping Noise Pollution with Mobile Phones, in: Proceedings of the 4th International Symposium on Information Technologies in Environmental Engineering (ITEE), 2009, pp. 215–228.

[40] H. Lu, W. Pan, N. D. Lane, T. Choudhury, A. T. Campbell, SoundSense: Scalable Sound Sensing for People-centric Applications on Mobile Phones, in: Proceedings of the 7th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys), 2009, pp. 165–178.

[41] X. Bao, R. R. Choudhury, MoVi: Mobile Phone based Video Highlights via Collaborative Sensing, in: Proceedings of the 8th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys), 2010, pp. 357–370.

[42] R. K. Rana, C. T. Chou, S. S. Kanhere, N. Bulusu, W. Hu, Ear-Phone: An End-to-end Participatory Urban Noise Mapping System, in: Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN), 2010, pp. 105–116.

[43] E. D'Hondt, M. Stevens, A. Jacobs, Participatory Noise Mapping Works! An Evaluation of Participatory Sensing as an Alternative to Standard Techniques for Environmental Monitoring, Pervasive and Mobile Computing 9 (5) (2013) 681–694.

[44] E. Niforatos, A. Vourvopoulos, M. Langheinrich, P. Campos, A. Doria, Atmos: A Hybrid Crowdsourcing Approach to Weather Estimation, in: Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp, Adjunct Publication), 2014, pp. 135–138.

[45] R. Ganti, I. Mohomed, R. Raghavendra, A. Ranganathan, Analysis of Data from a Taxi Cab Participatory Sensor Network, in: A. Puiatti, T. Gu (Eds.), Mobile and Ubiquitous Systems: Computing, Networking, and Services, Vol. 104 of Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Springer Berlin Heidelberg, 2012, pp. 197–208.

[46] P. Zhou, Y. Zheng, M. Li, How Long to Wait?: Predicting Bus Arrival Time with Mobile Phone Based Participatory Sensing, in: Proceedings of the 10th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys), 2012, pp. 379–392.

[47] M. von Kaenel, P. Sommer, R. Wattenhofer, Ikarus: Large-Scale Participatory Sensing at High Altitudes, in: Proceedings of the 12th Workshop on Mobile Computing Systems and Applications (HotMobile), 2011, pp. 55–60.

[48] FitnessKeeper, Inc., RunKeeper - GPS Track Run Walk, Online: https://play.google.com/store/apps/details?id=com.fitnesskeeper.runkeeper.pro (accessed in 02.2015).

[49] Endomondo.com, Endomondo, Online: https://play.google.com/store/apps/details?id=com.endomondo.android&hl=de (accessed in 02.2015).

[50] Nike, Inc., Nike+ Running, Online: https://play.google.com/store/apps/details?id=com.nike.plusgps&hl=de (accessed in 02.2015).

[51] MyFitnessPal, Inc., Calorie Counter - MyFitnessPal, Online: https://play.google.com/store/apps/details?id=com.myfitnesspal.android&rdid=com.myfitnesspal.android (accessed in 02.2015).

[52] Fitbit, Inc., Fitbit, Online: http://www.fitbit.com (accessed in 02.2015).

[53] Jawbone, Inc., Jawbone Up, Online: https://jawbone.com/up (accessed in 02.2015).

[54] Nike, Inc., Nike+ Fuelband SE, Online: www.nike.com (accessed in 02.2015).

[55] B. Dolan, Fitbit, Jawbone, Nike had 97 Percent of Fitness Tracker Retail Sales in 2013, Online: http://mobihealthnews.com (accessed in 02.2015) (2014).

[56] G. Wolf, Quantified Self, Online: http://antephase.com/quantifiedself (accessed in 02.2015).

[57] M. Swan, Health 2050: the Realization of Personalized Medicine through Crowdsourcing, the Quantified Self, and the Participatory Biocitizen, Journal of Personalized Medicine 2 (3) (2012) 93–118.

[58] M. Swan, Sensor mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0, Journal of Sensor and Actuator Networks 1 (3) (2012) 217–253.

[59] J. R. Whitson, Gaming the Quantified Self, Surveillance & Society 11 (1/2) (2013) 163–176.

[60] wer denkt was GmbH, AppJobber, Online: `http://en.appjobber.com` (accessed in 02.2015).

[61] D. Christin, A. Reinhardt, S. S. Kanhere, M. Hollick, A Survey on Privacy in Mobile Participatory Sensing Applications, Journal of Systems and Software (JSS) 84 (11) (2011) 1928–1946.

[62] J. Krumm, Inference Attacks on Location Tracks, in: Proceedings of the 5th IEEE International Conference on Pervasive Computing (Pervasive), 2007, pp. 127–143.

[63] Y.-A. de Montjoye, C. A. Hidalgo, M. Verleysen, V. D. Blondel, Unique in the Crowd: The Privacy Bounds of Human Mobility, Scientific reports 3.

[64] J. R. Kwapisz, G. M. Weiss, S. A. Moore, Activity Recognition using Cell Phone Accelerometers, SIGKDD Explorations Newsletter 12 (2011) 74–82.

[65] M. O. Derawi, C. Nickel, P. Bours, C. Busch, Unobtrusive User-authentication on Mobile Phones using Biometric Gait, in: Proceeding of the 6th IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010, pp. 306–311.

[66] L. Cai, H. Chen, TouchLogger: Inferring Keystrokes On Touch Screen From Smartphone Motion, in: Proceedings of the 6th USENIX Conference on Hot Topics in Security (HotSec), 2011, pp. 9–9.

[67] J. Han, E. Owusu, L. Nguyen, A. Perrig, J. Zhang, ACComplice: Location Inference using Accelerometers on Smartphones, in: 4th International Conference on Communication Systems and Networks (COMSNETS), 2012, pp. 1–9.

[68] N. D. Lane, J. Xie, T. Moscibroda, F. Zhao, On the Feasibility of User Deanonymization from Shared Mobile Sensor Data, in: Proceedings of the 3rd International Workshop on Sensing Applications on Mobile Phones (PhoneSense), 2012, pp. 3:1–3:5.

[69] T. Giannetsos, S. Gisdakis, P. Papadimitratos, Trustworthy People-Centric Sensing: Privacy, Security and User Incentives Road-map, in: Proceedings of the 13th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET), 2014, pp. 39–46.

[70] E. De Cristofaro, R. Di Pietro, Preserving Query Privacy in Urban Sensing Systems, in: Proceedings of the 13th International Conference on Distributed Computing and Networking (ICDCN), 2012, pp. 218–233.

[71] E. De Cristofaro, R. Di Pietro, Adversaries and Countermeasures in Privacy-Enhanced Urban Sensing Systems, IEEE Systems Journal 7 (2) (2013) 311–322.

[72] I. Rodhe, C. Rohner, E. C.-H. Ngai, On Location Privacy and Quality of Information in Participatory Sensing, in: Proceedings of the 8th ACM Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet), 2012, pp. 55–62.

[73] E. De Cristofaro, C. Soriente, Short Paper: PEPSI—Privacy-enhanced Participatory Sensing Infrastructure, in: Proceedings of the 4th ACM Conference on Wireless Network Security (WiSec), 2011, pp. 23–28.

[74] E. De Cristofaro, C. Soriente, Extended Capabilities for a Privacy-Enhanced Participatory Sensing Infrastructure (PEPSI), IEEE Transactions on Information Forensics and Security 8 (12) (2013) 2021–2033.

[75] E. De Cristofaro, C. Soriente, Participatory Privacy: Enabling Privacy in Participatory Sensing, IEEE Network 27 (1) (2013) 32–36.

[76] A. Kapadia, D. Kotz, N. Triandopoulos, Opportunistic Sensing: Security Challenges for the New Paradigm, in: Proceedings of the 1st International Conference on Communication Systems and Networks (COMNETS), 2009, pp. 1–10.

[77] M. Shin, C. Cornelius, D. Peebles, A. Kapadia, D. Kotz, N. Triandopoulos, AnonySense: A System for Anonymous Opportunistic Sensing, Journal of Pervasive and Mobile Computing 7 (1) (2010) 16–30.

[78] L. Kazemi, C. Shahabi, A Privacy-aware Framework for Participatory Sensing, ACM SIGKDD Explorations Newsletter 13 (1) (2011) 43–51.

[79] L. Kazemi, C. Shahabi, Towards Preserving Privacy in Participatory Sensing, in: Proceedings of the 9th IEEE International Conference on Pervasive Computing and Communications (PERCOM Workshops), 2011, pp. 328–331.

[80] L. Kazemi, C. Shahabi, TAPAS: Trustworthy Privacy-aware Participatory Sensing, Knowledge and Information Systems 37 (1) (2013) 105–128.

[81] K. Vu, R. Zheng, J. Gao, Efficient Algorithms for K-anonymous Location Privacy in Participatory Sensing, in: Proceedings of the 31th IEEE Conference on Computer Communications (INFOCOM), 2012, pp. 2399–2407.

[82] H. To, G. Ghinita, C. Shahabi, A Framework for Protecting Worker Location Privacy in Spatial Crowdsourcing, Proceedings of the Very Large Database Endowment (PVLDB) 7 (10) (2014) 919–930.

[83] I. Krontiris, T. Dimitriou, Privacy-respecting Discovery of Data Providers in Crowd-sensing Applications, in: Proceedings of the 9th IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS), 2013, pp. 249–257.

[84] D. Christin, A. Reinhardt, M. Hollick, K. Trumpold, Exploring User Preferences for Privacy Interfaces in Mobile Sensing Applications, in: Proceedings of 11th ACM International Conference on Mobile and Ubiquitous Multimedia (MUM), 2012, pp. 14:1–14:10.

[85] K. Wiesner, S. Feld, F. Dorfmeister, C. Linnhoff-Popien, Right to Silence: Establishing Map-based Silent Zones for Participatory Sensing, in: Proceedings of the 9th IEEE International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2014, pp. 1–6.

[86] S. Pidcock, R. Smits, U. Hengartner, I. Goldberg, Notisense: An Urban Sensing Notification System to Improve Bystander Privacy, in: Proceedings of the 2nd International Workshop on Sensing Applications on Mobile Phones (PhoneSense), 2011, pp. 1–5.

[87] D. Biswas, K. Vidyasankar, Privacy Preserving Profiling for Mobile Services, Procedia Computer Science 10 (0) (2012) 569–576.

[88] C.-J. Wang, W.-S. Ku, Anonymous Sensory Data Collection Approach for Mobile Participatory Sensing, in: Proceedings of the 28th IEEE International Conference on Data Engineering Workshops (ICDEW), 2012, pp. 220–227.

[89] D. Christin, J. Guillemet, A. Reinhardt, M. Hollick, S. S. Kanhere, Privacy-preserving Collaborative Path Hiding for Participatory Sensing Applications, in: Proceedings of the 8th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS), 2011, pp. 341–350.

[90] D. Christin, A. Reinhardt, M. Hollick, On the Efficiency of Privacy-Preserving Path Hiding for Mobile Sensing Applications, in: Proceedings of the 38th IEEE Conference on Local Computer Networks (LCN), 2013, pp. 846–854.

[91] J. Shi, R. Zhang, Y. Liu, Y. Zhang, PriSense: Privacy-preserving Data Aggregation in People-centric Urban Sensing Systems, in: Proceedings of

the 29th IEEE International Conference on Computer Communications (INFOCOM), 2010, pp. 1–9.

[92] F. Qiu, F. Wu, G. Chen, SLICER: A Slicing-Based K-Anonymous Privacy Preserving Scheme for Participatory Sensing, in: Proceedings of the 10th IEEE International Conference on Mobile Ad-Hoc and Sensor Systems (MASS), 2013, pp. 113–121.

[93] S. Gao, J. Ma, W. Shi, G. Zhan, Towards Location and Trajectory Privacy Protection in Participatory Sensing, in: Proceedings of the 3rd International Conference on Mobile Computing, Applications, and Services (MobiCASE), 2011, pp. 381–386.

[94] S. Gao, J. Ma, W. Shi, G. Zhan, C. Sun, TrPF: A Trajectory Privacy-Preserving Framework for Participatory Sensing, IEEE Transactions on Information Forensics and Security 8 (6) (2013) 874–887.

[95] M. Murshed, A. Iqbal, T. Sabrina, K. M. Alam, A Subset Coding Based k-Anonymization Technique to Trade-Off Location Privacy and Data Integrity in Participatory Sensing Systems, in: Proceedings of the 10th IEEE International Symposium on Network Computing and Applications (NCA), 2011, pp. 107–114.

[96] I. Boutsis, V. Kalogeraki, Privacy Preservation for Participatory Sensing Data, in: Proceedings of the 11th IEEE International Conference on Pervasive Computing and Communications (PerCom), 2013, pp. 103–113.

[97] M.-R. Ra, B. Liu, T. F. La Porta, R. Govindan, Medusa: A Programming Framework for Crowd-sensing Applications, in: Proceedings of the 10th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys), 2012, pp. 337–350.

[98] D. Christin, C. Roßkopf, M. Hollick, L. A. Martucci, S. S. Kanhere, IncogniSense: An Anonymity-preserving Reputation Framework for Participatory Sensing Applications, in: Proceedings of the 10th IEEE Interna-

tional Conference on Pervasive Computing and Communications (PerCom), 2012, pp. 135–143.

[99] D. Christin, C. Roßkopf, M. Hollick, L. A. Martucci, S. S. Kanhere, IncogniSense: An Anonymity-preserving Reputation Framework for Participatory Sensing Applications, Pervasive and Mobile Computing (PMC) 9 (3) (2013) 353–371.

[100] K. L. Huang, S. S. Kanhere, W. Hu, A Privacy-preserving Reputation System for Participatory Sensing, in: Proceedings of the 37th IEEE Conference on Local Computer Networks (LCN), 2012, pp. 10–18.

[101] Q. Li, G. Cao, Providing Privacy-aware Incentives for Mobile Sensing, in: Proceedings of the 11th IEEE International Conference on Pervasive Computing and Communications (PerCom), IEEE, 2013, pp. 76–84.

[102] J. Zhang, J. Ma, W. Wang, Y. Liu, A Novel Privacy Protection Scheme for Participatory Sensing with Incentives, in: Proceedings of the 2nd IEEE International Conference on Cloud Computing and Intelligent Systems (CCIS), 2012, pp. 1017–1021.

[103] S. Gisdakis, T. Giannetsos, P. Papadimitratos, SPPEAR: Security and Privacy-preserving Architecture for Participatory-sensing Applications, in: Proceedings of the 7th ACM Conference on Security and Privacy in Wireless Mobile Networks (WiSec), 2014, pp. 39–50.

[104] X. O. Wang, W. Cheng, P. Mohapatra, T. Abdelzaher, Enabling Reputation and Trust in Privacy-Preserving Mobile Sensing, IEEE Transactions on Mobile Computing (2013) 1–14.

[105] X. O. Wang, W. Cheng, P. Mohapatra, T. Abdelzaher, ARTSense: Anonymous Reputation and Trust in Participatory Sensing, in: Proceedings of the 32th IEEE Conference on Computer Communications (INFOCOM), IEEE, 2013, pp. 2517–2525.

[106] A. Michalas, N. Komninos, The Lord of the Sense: A Privacy Preserving Reputation System for Participatory Sensing Applications, in: Proceedings of the 19th IEEE Symposium on Computers and Communication (ISCC), 2014, pp. 1–6.

[107] S. Chakraborty, K. R. Raghavan, M. P. Johnson, M. B. Srivastava, A Framework for Context-aware Privacy of Sensor Data on Mobile Systems, in: Proceedings of the 14th Workshop on Mobile Computing Systems and Applications (HotMobile), 2013, pp. 11:1–11:6.

[108] B. Agir, T. G. Papaioannou, R. Narendula, K. Aberer, J.-P. Hubaux, User-side Adaptive Protection of Location Privacy in Participatory Sensing, Geoinformatica 18 (1) (2014) 165–191.

[109] K. Dong, T. Gu, X. Tao, J. Lu, Privacy Protection in Participatory Sensing Applications Requiring Fine-Grained Locations, in: Proceedings of the 16th IEEE International Conference on Parallel and Distributed Systems (ICPADS), 2010, pp. 9–16.

[110] I. J. Vergara-Laurens, D. Mendez, M. A. Labrador, Privacy, Quality of Information, and Energy Consumption in Participatory Sensing Systems, in: Proceedings of the 12th IEEE International Conference on Pervasive Computing and Communications (PerCom), 2014, pp. 199–207.

[111] F. Zhang, L. He, W. He, X. Liu, Data Perturbation with State-dependent Noise for Participatory Sensing, in: Proceedings of the 31th IEEE Conference on Computer Communications (INFOCOM), 2012, pp. 2246–2254.

[112] J. Zhu, K.-H. Kim, P. Mohapatra, P. Congdon, An Adaptive Privacy-preserving Scheme for Location Tracking of a Mobile User, in: Proceedings of the 10th IEEE International Conference on Sensing, Communication, and Networking (SECON), IEEE, 2013, pp. 140–148.

[113] M. Groat, B. Edwards, J. Horey, W. He, S. Forrest, Enhancing Privacy in Participatory Sensing Applications with Multidimensional Data, in: Pro-

ceedings of the 10th IEEE International Conference on Pervasive Computing and Communications (PerCom), 2012, pp. 144–152.

[114] G. Drosatos, P. S. Efraimidis, I. N. Athanasiadis, E. D'Hondt, M. Stevens, A Privacy-preserving Cloud Computing System for Creating Participatory Noise Maps, in: Proceedings of the 36th IEEE Annual Computer Software and Applications Conference (COMPSAC), IEEE, 2012, pp. 581–586.

[115] G. Drosatos, P. S. Efraimidis, I. N. Athanasiadis, M. Stevens, E. D'Hondt, Privacy-preserving Computation of Participatory Noise Maps in the Cloud, Journal of Systems and Software 92 (0) (2014) 170–183.

[116] Q. Li, G. Cao, Efficient and Privacy-preserving Data Aggregation in Mobile Sensing, in: Proceedings of the 20th IEEE International Conference on Network Protocols (ICNP), 2012, pp. 1–10.

[117] Q. Li, G. Cao, Efficient Privacy-Preserving Stream Aggregation in Mobile Sensing with Low Aggregation Error, in: E. De Cristofaro, M. Wright (Eds.), Privacy Enhancing Technologies, Vol. 7981 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2013, pp. 60–81.

[118] R. Zhang, J. Shi, Y. Zhang, C. Zhang, Verifiable Privacy-Preserving Aggregation in People-Centric Urban Sensing Systems, IEEE Journal on Selected Areas in Communications 31 (9) (2013) 268–278.

[119] X. Chen, X. Wu, X.-Y. Li, Y. He, Y. Liu, Privacy-preserving High-quality Map Generation with Participatory Sensing, in: Proceedings of the 33th IEEE Conference on Computer Communications (INFOCOM), 2014, pp. 2310–2318.

[120] H. Choi, S. Chakraborty, Z. Charbiwala, M. Srivastava, SensorSafe: A Framework for Privacy-Preserving Management of Personal Sensory Information, in: W. Jonker, M. Petković (Eds.), Secure Data Management, Vol. 6933 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2011, pp. 85–100.

[121] H. Choi, S. Chakraborty, M. B. Srivastava, Design and Evaluation of SensorSafe: A Framework for Achieving Behavioral Privacy in Sharing Personal Sensory Information, in: Proceedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2012, pp. 1004–1011.

[122] S. Chakraborty, H. Choi, M. B. Srivastava, Demystifying Privacy in Sensory Data: A QoI based Approach, in: Proceedings of the 9th Annual IEEE International Conference on Pervasive Computing and Communications (PerCom Workshops), 2011, pp. 38–43.

[123] S. Chakraborty, Z. Charbiwala, H. Choi, K. R. Raghavan, M. B. Srivastava, Balancing Behavioral Privacy and Information Utility in Sensory Data Flows, Pervasive and Mobile Computing 8 (3) (2012) 331–345.

[124] M. Y. Mun, D. H. Kim, K. Shilton, D. Estrin, M. Hansen, R. Govindan, PDVLoc: A Personal Data Vault for Controlled Location Data Sharing, ACM Transactions Sensor Networks 10 (4) (2014) 58:1–58:29.

[125] L. Becchetti, L. Filipponi, A. Vitaletti, Privacy Support in People-centric Sensing, Journal of Communications 7 (8) (2012) 606–621.

[126] T. Dimitriou, I. Krontiris, A. Sabouri, PEPPeR: A Querier's Privacy Enhancing Protocol for PaRticipatory Sensing, in: A. Schmidt, G. Russello, I. Krontiris, S. Lian (Eds.), Security and Privacy in Mobile Information and Communication Systems, Vol. 107 of Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Springer Berlin Heidelberg, 2012, pp. 93–106.

[127] L. Pournajaf, L. Xiong, V. Sunderam, S. Goryczka, Spatial Task Assignment for Crowd Sensing with Cloaked Locations, in: Proceedings of the 15th IEEE International Conference on Mobile Data Management (MDM), Vol. 1, 2014, pp. 73–82.

[128] C. Dwork, Differential Privacy, in: M. Bugliesi, B. Preneel, V. Sassone, I. Wegener (Eds.), Automata, Languages and Programming, Vol. 4052 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2006, pp. 1–12.

[129] D. Christin, M. Michalak, M. Hollick, Raising User Awareness about Privacy Threats in Participatory Sensing Applications through Graphical Warnings, in: Proceedings of the 11th International Conference on Advances in Mobile Computing and Multimedia (MoMM), 2013, pp. 445–454.

[130] D. Chaum, Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, Communications of the ACM 24 (2) (1981) 84–90.

[131] A. Beresford, F. Stajano, Location Privacy in Pervasive Computing, IEEE Pervasive Computing 2 (1) (2003) 46–55.

[132] D. Christin, D. R. Pons-Sorolla, M. Hollick, S. S. Kanhere, TrustMeter: A Trust Assessment Framework for Collaborative Path Hiding in Participatory Sensing Applications, in: Proceedings of the 9th IEEE International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2014, pp. 1–6.

[133] D. Christin, F. Engelmann, M. Hollick, Usable Privacy for Mobile Sensing Applications, in: D. Naccache, D. Sauveron (Eds.), Information Security Theory and Practice. Securing the Internet of Things, Vol. 8501 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2014, pp. 92–107.

[134] K. Shilton, J. A. Burke, D. Estrin, M. Hansen, M. B. Srivastava, Participatory Privacy in Urban Sensing, in: Proceedings of the International Workshop on Mobile Devices and Urban Sensing (MODUS), 2008, pp. 1–7.

[135] K. Shilton, K. E. Martin, Mobile Privacy Expectations in Context, in: Proceedings of the 41st Research Conference on Communication, Information and Internet Policy (TPRC), 2013, pp. 1–27.

[136] D. Christin, C. Büchner, N. Leibecke, What's the Value of Your Privacy? Exploring Factors That Influence Privacy-sensitive Contributions to Participatory Sensing Applications, in: Proceedings of the IEEE Workshop on Privacy and Anonymity for the Digital Economy (LCN Workshops), 2013, pp. 946–951.

[137] I. J. Vergara-Laurens, D. Mendez-Chaves, M. A. Labrador, On the Interactions between Privacy-Preserving, Incentive, and Inference Mechanisms in Participatory Sensing Systems, in: J. Lopez, X. Huang, R. Sandhu (Eds.), Network and System Security, Vol. 7873 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2013, pp. 614–620.

[138] M. L. Damiani, Location Privacy Models in Mobile Applications: Conceptual View and Research Directions, GeoInformatica (2014) 1–24.