

RESEARCH ARTICLE

People-Centric Sensing in Assistive Healthcare: Privacy Challenges and Directions

Thanassis Giannetsos^{1*}, Tassos Dimitriou¹, Neeli R. Prasad²

¹ Athens Information Technology, 19.5 km Markopoulo Ave., Athens, Greece. E-mail: agia@ait.edu.gr & tdim@ait.edu.gr

² Department of Communication, Aalborg University, Fr. Bajers Vej 7A5, DK-9220, Denmark. E-mail: np@es.aau.dk

ABSTRACT

As the domains of pervasive computing and sensor networking are expanding, there is an ongoing trend towards assistive living and healthcare support environments that can effectively assimilate these technologies according to human needs. Most of the existing research in assistive healthcare follows a more *passive* approach and has focused on collecting and processing data using a static-topology and an application-aware infrastructure. However, with the technological advances in sensing, computation, storage, and communications, a new era is about to emerge changing the traditional view of sensor-based assistive environments where people are passive data consumers, with one where people carry mobile sensing elements involving large volumes of data related to everyday human activities. This evolution will be driven by *people-centric sensing* and will turn mobile phones into global mobile sensing devices enabling thousands new personal, social, and public sensing applications. In this paper, we discuss our vision for people-centric sensing in assistive healthcare environments and study the security challenges it brings. This highly dynamic and mobile setting presents new challenges for information security, data privacy and ethics, caused by the ubiquitous nature of data traces originating from sensors carried by people. We aim to instigate discussion on these critical issues because people-centric sensing will never succeed without adequate provisions on security and privacy. To that end, we discuss the latest advances in security and privacy protection strategies that hold promise in this new exciting paradigm. We hope this work will better highlight the need for privacy in people-centric sensing applications and spawn further research in this area.

Copyright © 2010 John Wiley & Sons, Ltd.

KEYWORDS

Participatory Sensing, Assistive Healthcare, Mobile Handsets, Security and Privacy Policies, Location and Context-Awareness

* Correspondence

Athens Information Technology, 19.5 km Markopoulo Ave., Athens, Greece. E-mail: agia@ait.edu.gr

Received ...

1. INTRODUCTION

Sensor networks provide tremendous potential for information collection and processing in a variety of application domains. A decade ago, the first generation of sensor nodes facilitated the genesis of wireless sensor networks as they exist today: small resource-constrained embedded devices that communicate via low-power, low-bandwidth radio, capable of performing simple sensing tasks. A first set of scenarios for these networks included stationary nodes sensing ephemeral features of the environment, like temperature, noise, air pollution, etc. By continuously monitoring these surrounding attributes, they solved relatively small-scale specialized problems such as forest monitoring, preventative maintenance, etc.

Although these problems and applications remain important, the recent advances in pervasive and ubiquitous computing led to new exciting applications for sensor networks involving their use in assistive healthcare environments. For example, in a hospital, outfitting every patient with tiny, wearable vital sign sensors would allow doctors to continuously monitor the status of their patients (e.g., MobiCare [1], CodeBlue [2], WW-BAN [3], and HealthGear [4]). Similarly, in an emergency or disaster scenario, the same technology would enable medics to more effectively care for people casualties. Additionally, in assistive environments, sensor-based monitoring can be proved a valuable tool for those who may have physical or cognitive impairment. It is an ideal technology that provides most direct and effective information about users' location and activities [5]. In general, wireless sensors can

Table I. Traditional Sensor Networks vs. People-Centric Sensing

Traditional Sensor Net.	People-Centric Sensing
Specially designed deployed hardware	Leveraging available devices
Fully automatic & standalone systems	Humans in the loop
Thousands of small devices	Systems of heterogeneous devices
Fixed, Static Deployment	Mobility

replace existing wired systems for many specific clinical and healthcare applications.

Despite the increased interest in this area, a significant gap remains between existing sensor network designs and the requirements of assistive healthcare environments. This is due to the resource constraints and memory limitations that characterize sensor networks. Most of them are intended for deployments of stationary nodes that transmit data at relatively low data rates, with a focus on best-effort data collection at a central base station. In contrast, assistive healthcare requires *high data rates, reliable communication and multiple receivers*. Moreover, unlike many sensor network applications, healthcare monitoring cannot make use of traditional network protocols since it generally assumes high *mobility* of the people carrying the wireless devices.

These limitations in combination with the technological advances in sensing, computation, storage, and communication has opened the door to a new world of possibilities. Assistive and healthcare environments will eventually incorporate the latest pervasive and ubiquitous technologies in order to provide a viable alternative to “traditional” assistive living. This new trend will change the traditional view of sensor-based assistive environments where people are *passive* data consumers that simply interact with physically embedded static sensor webs, with one where people carry mobile sensing elements involving the collection, storage, processing and fusion of large volumes of data related to everyday human activities. This evolution is driven by the miniaturization and introduction of sensors into popular electronic devices like mobile phones and PDAs. With wireless sensor platforms in the hands of thousands, we can expect sensor networks to address *urban-scale* problems like public health monitoring and personal well-being improvement. For example, participatory sensing can facilitate the anticipation and tracking of disease outbreaks across populations [6]. At the same time, people as individuals, can apply these new sensing networks to applications with a more personal focus [7, 8].

Such systems, often referred to as *urban sensing* or *people-centric sensing* [9] systems, come to complement previous efforts on extending the possibilities of wireless sensor networks by taking advantage of the large scale of sensors already existing in our hands (as seen in

Table I). These systems aim at daily life applications, employing the mobile devices people already carry for sensing information directly or indirectly related to human activity, as well as aspects of the environment around them.

These ubiquitous devices are increasingly capable of capturing and transmitting image, acoustic, location, and other data, interactively or autonomously. They can become the best platform for coordinated investigation of the environment and human activity [10, 11, 12] by enabling users to gather, analyze, and share local knowledge. With these capabilities in mind, and new network architectures for enhancing data credibility, quality, privacy, and “shareability”, they can encourage people participation at personal, social and urban scales.

In a people-centric system, humans, rather than machines, are the focal point of the sensing infrastructure enabling sensing coverage of large public spaces over time and letting individuals, as *sensing device custodians*, collect targeted information about their daily patterns and interactions. However, this new brand of sensing induces a different set of trade-offs than in much of the prior work on sensor networks, requiring new thoughts on the communication and network architectures. Never before has sensing been so close to the public, and so intermixed in their daily lives. Therefore, these new capabilities pose different challenges for information security and privacy and present significant technical and ethical issues.

First, applications may deal with personal information, requiring a deeper attention to *privacy* and *anonymity*. Data traces can easily document and quantify habits, routines, and personal associations. Second, motivating user participation within the fast-paced development of participatory urban sensing is both challenging and important. We believe that in order to ensure people’s participation, we must provide solution to the following trust concerns: *content reliability* (How do you have confidence that the published data is indeed what was sensed?) and *content protection* (How to ensure that only authorized entities can access published data?). Finally, modified assumptions about device and network capabilities (including high mobility, strong but not continuous connectivity, and relatively plentiful power) lead to new opportunities and require different security solutions. Thus, current security mechanisms that focus on resource-constrained devices, static network deployments, etc., are not suitable for the envisioned people-centric sensing applications.

1.1. Our Contribution

Given the increase interest in this emerging area of participatory sensing applications, new challenging questions will be raised whose answers can potentially affect system designs and architectures. In this paper, we focus on an important class of these applications which can be incorporated in assistive healthcare environments. In these settings, sensor devices will (i) be highly mobile, (ii) have limited resources, but not severely so, and, most

importantly, *(iii)* they will be carried by people, thus introducing privacy concerns as well as new adversarial threat models.

We discuss how this evolution may change “traditional” assistive living systems and we try to envisage the next generation of public/personal healthcare support. We survey all the security and privacy challenges involved, and try to identify some key solution concepts. We make the case for trustworthy participatory sensing and motivate the problems of data protection, shareability, and confidentiality. In general, we hope this work will instigate discussion on these critical issues, and encourage application and system designers to embed more robust security and privacy features prior to deploying healthcare systems. We believe that people-centric sensing will never succeed without adequate provisions on security and privacy.

1.2. Paper Organization

The remainder of this paper is organized as follows. Section 2 outlines the designs adopted in “traditional” assistive healthcare support systems, their challenges and the most important solution concepts currently used. In Section 3, we overview people-centric sensing, identify the key features driving this ongoing trend, and discuss certain applications enabled by this new form of sensing. In Section 4, we describe what we believe to be the new challenges in the area and discuss the latest advances along with some conceptual solutions. Finally, Section 5 concludes the paper.

2. BACKGROUND ON TRADITIONAL ASSISTIVE HEALTHCARE SYSTEMS

Assistive-living environments and healthcare support have been an emerging area of research for the past five years. This fast-paced development is mainly due to two reasons: *(i)* Continuing integration and miniaturization of sensors, processors, and radio devices, *(ii)* Rising demands for advanced assistive healthcare systems ranging from pivotal areas of elderly protection and clinical patient monitoring to much broader applications in military, preventive healthcare, and personal well-being improvement.

The benefit of using wireless sensors in assistive healthcare is threefold: First, they allow monitoring of the individual at home, so that the elderly or patients with chronic diseases can enjoy treatment and medical monitoring at their own environment [13]. Second, they substantially increase the efficiency of treatments inside the hospital environment. Emergency and intensive medical care can all benefit from continuous vital sign monitoring, e.g. immediate notification of patient deterioration. Sensor data can be integrated into electronic patient care records and retrieved for later analysis. This results in enhanced decision making for diagnostics, observation and patient treatment.

Most importantly, though, what makes sensor networks the most appropriate technology for assistive living are their unique characteristics. The advantages for smart healthcare systems are numerous, as they provide the following important properties:

- **Portability and unobtrusiveness.** Small devices collect data and communicate wirelessly, operating with minimal patient input. They may be carried on the body or be embedded in the environment. Unobtrusiveness enhances patient acceptance since monitoring is performed in their living space which is more convenient.
- **Ease of deployment and scalability.** Devices can be deployed in potentially large quantities with dramatically less complexity and cost compared to wired networks. They are usually placed in assistive living spaces and they are turned on, self-organized and calibrated automatically.
- **Real-time operation.** Patient data can be monitored continuously, allowing real-time response by emergency or healthcare workers. Also, individual sensors can conserve energy through smart power management and on-demand activation.
- **Reconfiguration, adaptability and self-organization.** Since there is no fixed installation, adding and removing sensors instantly reconfigures the network. Healthcare workers may re-target the mission of the network as individual needs change.

All the above described features meet the requirements for assistive healthcare environments. Thus, existing systems adopt these design attributes in order to form ad hoc networks, with reliable communications, capable of relaying continuous vital sign data to the receiving devices of healthcare workers. Such systems can be translated directly into hospital and living space settings where wired monitoring is cumbersome and obstructs the caregiver’s access to the patient. There are a number of sophisticated assistive healthcare sensor network systems that consist of multiple heterogeneous sensors, adopt hierarchical architectures for real-time sensor management, and integrate body sensors with other environmental sensors. A brief overview of the most important ones can be found in the next section.

2.1. Assistive-Living and Healthcare Support Systems

A number of research projects and commercially available systems already exist that explore the use of sensor networks in assistive healthcare environments. Traditional ones mainly involve single wearable sensors, such as fall detection [14, 15], walk and gait-phase detection [16], and pulse-oximetry monitoring [17]. VivoMetrics has developed LifeShirt [18], a washable lightweight vest that includes respiratory rate sensors, one-lead ECG for heart rate measurement and an accelerometer for activity monitoring. Also, BodyMedia has developed the

Table II. Threat Model considered for Assistive Healthcare systems

Risk Type	Threats	Risk Level	Risk Response	Countermeasures
Integrity	<i>Spoofing, Replay, Sybil</i> : Adversaries contribute bogus sensory data	High	Prevent false data injection	Data validation, Keyed secure hash function, Digital signature
Confidentiality, Privacy	<i>Eavesdropping, Message Disclosure</i> : Gain access to sensitive information	High	Prevent data decoding	Link/Network layer encryption, Access Control
Authentication	<i>Message modification, Node compromise</i> : Unauthorized access to health data	High	Set up a trust node scheme	Random key distribution, Node revocation, Inconsistency detection
Availability	<i>DoS Attack, Selective Forwarding</i> : Disrupt operation or drop reports of events	High	Priority in node service, Msg Sequences	Intrusion detection, Redundancy

SenseWear [19] armband that has multiple sensors (skin and near-body temperature, two-axis accelerometer, etc.) to continuously collect physiological data for a few days at a time. Once the data is collected and processed by their proprietary software, these systems can extract information about the individuals’ lifestyle.

Moving on to more sophisticated solutions that focus on developing robust and scalable infrastructures for deploying sensor networks in a range of medical settings, we come across HealthGear [4]. HealthGear is a real-time wearable system for monitoring, visualizing and analyzing physiological signals. It uses an oximeter to constantly monitor and analyze the user’s blood oxygen level (SpO_2), heart rate and plethysmographic signal in a lightweight fashion. It consists of a set of non-invasive physiological sensors wirelessly connected via Bluetooth to a cell phone which stores, transmits and analyzes the collected data, and presents it to the user in an intelligible way. A relevant project to the HealthGear prototype is AMON [20], a wearable (wrist-worn) medical monitoring and alert system targeting high-risk cardiac/respiratory patients who would be confined to the hospital or their homes. The system includes continuous collection and evaluation of multiple vital signals, medical emergency detection and GSM-based secure cellular connection to a medical center.

Another interesting project is LifeGuard [21], a multiparameter wearable physiological monitoring system for space and terrestrial applications. It’s core element is a crew physiologic observation device which is capable of monitoring respiration rate, heart rate, oxygen saturation, body temperature, blood pressure and body movement. In [3], the development of a prototype wearable wireless body area network (WW-BAN) is described. The proposed system consists of several motion sensors that monitor the users overall activity and an ECG sensor for monitoring heart activity. Similarly, researchers in Harvard university have developed CodeBlue [2], a medical sensor network platform for multipatient monitoring environments. This project enhances first responders’ ability to assess patients on scene, ensures seamless transfer of data among

caregivers, and facilitates efficient allocation of hospital resources. Another interesting approach is to use camera-based monitoring in order to meet the important needs of the elderly or those who may have physical or cognitive impairment. In [5], the authors proposed Sensor-Integrated Camera Surveillance (SICS) for assistive living spaces. SICS uses wearable wireless sensors to locate moving subjects and automatically selects the camera covering the subject, allowing human operators to focus only on one screen to monitor an individual. Finally, a number of projects [22, 23] at the Heracleia Lab, at University of Texas Arlington, focus towards the provision of better medical services and also in monitoring people with chronic diseases and Alzheimer [24].

There is a lot of interest lately in developing environments utilizing various types of assistive technologies. Towards this direction, Vassis *et al.* [25] described a policy-based architecture that utilizes wireless sensor devices, advanced network topologies and software agents to enable remote monitoring of patients and elderly people. Combining the aforementioned technologies, the authors presented a software framework that is able to continuously monitor a patient’s condition and proceed, when necessary, with proper actions. Furthermore, in [26] the authors proposed a framework, targeting people with specific difficulties, that aims in the provision of advanced services towards the facilitation of access to information for specific groups of people. Their approach achieves location-independent information access, while with personalized services there is a capability to adjust the interfaces and contents to various demands of the participating user-groups. For a more complete survey of assistive healthcare systems, the reader is referred to [27].

2.2. Security and Privacy Challenges

The particular threats that an assistive healthcare environment has to face, focus on the challenges posed by the resource-constrained sensor devices used. As we described in previous sections, WSNs bring a number of improvements to healthcare, but, as they are deployed in

an exposed environment, they are the weakest link that needs to be protected. Interacting closely with both people and the surrounding physical environment leads to such a level of exposure that significantly increases security vulnerabilities in cases of improperly managed security.

More specifically, security and privacy threats can be categorized into outsider and insider attacks [28]. In an *outsider* attack, the adversary is not an authorized participant of the sensor network. Authentication and encryption techniques typically prevent such an attacker from gaining any special access to the sensory data. However, the intruder node can be used to launch attacks, like: (i) eavesdropping, where the attacker eavesdrops and records transmitted messages, (ii) denial of service attacks, where the adversary attempts to disrupt the network's operation, and (iii) replay attacks, where the attacker captures messages exchanged between legitimate nodes and replays them in order to change the aggregation results.

Perhaps more dangerous from a security point of view is an *insider* attack, where an adversary by physically capturing a node and reading its memory, can obtain its key material and behave like a legitimate node. Having access to cryptographic keys, the attacker can launch several kinds of attacks without easily being detected: (i) unauthorized access to health data, (ii) false data injection, where the attacker injects fake results which are significantly different from the true health data determined by the biosensors, (iii) selective reporting, where the attacker stalls the reports of events by dropping legitimate packets that pass through the compromised node, and (iv) alteration of health data of a patient, leading to incorrect diagnosis and treatment.

In general, threat analysis for assistive healthcare environments is based on these forms of active and passive attacks that try to compromise the system's information security profile. All health monitoring networks share interest in confidentiality, integrity, authentication, and availability. *Confidentiality* is defined as the assurance that information is accessible only to those authorized to have access to it. It is important in order to protect the secrecy of any sensed data and communication exchanges. *Integrity* and *authentication* are necessary to enable sensor nodes to detect modified, injected, or replayed packets. Finally, *availability* is defined as the correct and consistent operation of all network nodes as implied by the underlying protocols. In healthcare applications, keeping the network available for its intended use is essential. Thus, attacks like denial-of-service (DoS) that aim at bringing down the network itself may have serious consequences to the health and well being of people.

2.3. Security Solutions

Several security solutions have been proposed in protecting biomedical sensor networks. More attention has been given to robust and efficient key management schemes, which serve as the fundamental requirement in encryption and

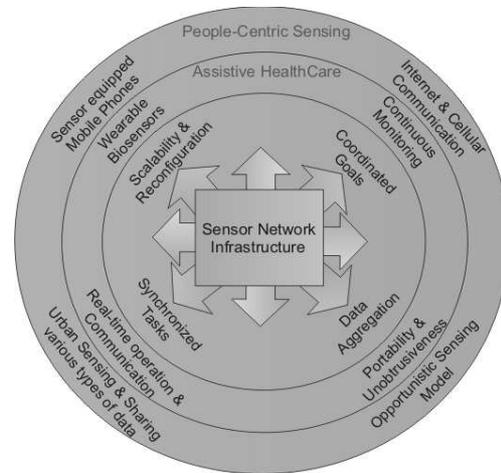


Figure 1. Moving on from traditional sensor networks and assistive healthcare systems to people-centric sensing

authentication. Table II summarizes all the security and privacy threats along with some possible countermeasures.

Existing work focuses on security mechanisms that can operate in resource-constrained environments such as sensor networks. For example, TinySec [29, 30] and its variants [31] is proposed as a solution to achieve link-layer encryption and authentication of sensitive data. It generates secure packets by encrypting data packets using a group key shared among nodes and calculating a MAC for the whole packet. As an alternative to TinySec, one could utilize hardware encryption by the ChipCon 2420 ZigBee compliant RF Transceiver. Based on AES encryption using 128-bit keys, the CC2420 can perform IEEE 802.15.4 MAC security operations, including counter (CTR) mode encryption and decryption, CBC-MAC authentication and CCM encryption plus authentication.

While encryption and authentication mechanisms provide a reasonable level of defense, they prove to be inefficient in preventing against insider attacks. The last resort is intrusion detection [32, 33], which can act as a second line of defense: it can *detect* third party break-in attempts, even if this particular attack has not been experienced before. Many researchers reference intrusion detection systems as a reliable solution for biomedical sensor networks [34, 35]. Other works have focused on secure routing techniques for static sensor networks [36, 37], secure data collection and aggregation [38, 39], and providing anonymity in location-based applications [40].

In general, the viability and long-term success of assistive healthcare networks depend upon addressing all the above described security threats successfully. An even greater challenge, however, is to *integrate assistive healthcare and people-centric sensing*. This is still an open research area with great interest on multi-fence security solutions that could be embedded into every component of the network in order to ensure privacy, integrity, and reliability of the entire system. The unique challenges

introduced by these next generation systems will be considered in the sections that follow.

3. BRIDGING ASSISTIVE HEALTHCARE AND PEOPLE-CENTRIC SENSING

Embedded wireless sensing already provides scientists and engineers unique insights into the physical and biological processes of an individual’s health monitoring status. Despite, however, the increased interest in this area, a significant gap remains between existing health monitoring designs and the requirements of assistive healthcare environments. Traditional systems are still limited to closed environments (hospital and living spaces) and they do not provide connectivity to global networks, thus degrading the level of usefulness in extreme situations like emergency care settings. Moreover, the special characteristics of various biosensors are specific to the system and change depending on application and deployment area. This results in developing from scratch certain processing tasks. For example, medical monitoring cannot make use of traditional in-network aggregation techniques since it is not meaningful to combine data from multiple patients.

All these limitations combined with the recent explosion of sensor-equipped mobile phone market, has opened the door to a new world of application possibilities (Figure 1). WSNs now can be leveraged to address urban-scale problems or provide global information access. This trend is also amplified by the need to achieve a more human centered vision of ubiquitous computing; *(i)* understand and support human daily life and activity, *(ii)* reinforce people’s social behavior by the creation and use of various devices that can provide interactive experiences to individuals in several ways, and *(iii)* manage in a skilful way all the devices that are connected to the network in order to provide a deeper everyday personal experience to the user.

People-centric sensing is a revolutionary paradigm of this ongoing trend that makes people the focal point of the sensing infrastructure. It allows them to *voluntarily* sense their environment using readily available sensor devices such as smart phones and share this information using existing cellular and Internet communication networks. It has tremendous potential because it harnesses the power of ordinary citizens to collect sensor data for applications spanning environmental monitoring, intelligent transportation, and, most importantly, public healthcare support which is often not cost-viable using dedicated sensing infrastructure.

We believe that participatory sensing will give rise to a host of new alternatives for assistive healthcare environments. Systems that will instrument the human body as an active mobile platform, will support persistent monitoring and sharing of data with everyone for the greater public good.

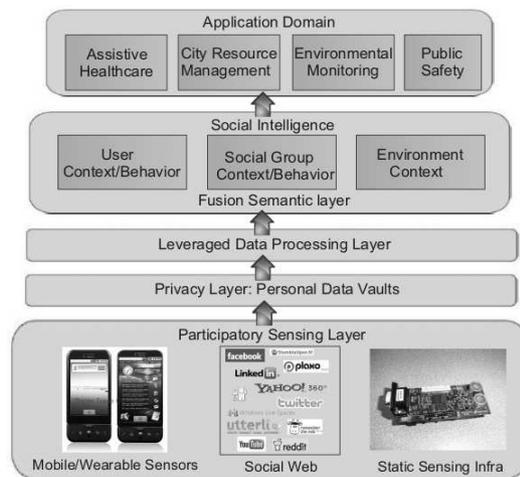


Figure 2. General architecture followed in People-Centric Sensing environments

3.1. Opportunistic People-Centric Sensing

People-centric sensing [9] lies at the intersection of several research domains, including sensor networking, ubiquitous computing, mobile computing, machine learning, human-computer interfacing, and social networking. Significant technological advancements made within each domain have driven this evolution, and research focusing on capitalizing these contributions is now emerging [41]. This new kind of sensing paradigm describes the process whereby individuals and communities use their mobile handsets and cloud services to collect and analyze systematic data for use in discovery. The convergence of technology and analytical innovation with a human-centered vision using mobile phones and online social networking, sets the stage for this technology to dramatically impact many aspects of our daily lives.

People-centric sensing differs from traditional sensor networks in that there is typically no single data producer. In an urban setting, for example, one could use millions of personal mobile phones, and a pervasive wireless-network infrastructure, to collect sensor data on a grand scale without the need of deploying thousands static sensors. Thus, many researchers proposed the *opportunistic-sensing* model, in which people volunteer their mobile devices to transparently collect sensor data as they go about their daily life. In the opportunistic-sensing model, sensor nodes are carried by people and therefore are conceptually tied to specific individuals. The sensors are inherently mobile and the sensor data is necessarily “people-centric”; that is, sensing not only the surrounding environment, but also aspects of the individual. For example, in assistive healthcare applications, people could produce data regarding their physical condition such as heart rate, body temperature, etc.

While these new aspects bring forth an amazing domain of new applications, they also present significant

security and privacy challenges. For instance, as in any participatory system, people-centric sensing is vulnerable to data crafting and sharing of incorrect information. Moreover, data producers and consumers are different autonomous entities. Thus, they may want to restrict whom they share their data with. A better description of all the challenges posed by this new technology, can be found in Section 4.

The essential technical components that enable the viability of such systems can be seen in Figure 2, which depicts a general architecture that is usually adopted in people-centric sensing systems. They consist of five layers [42]:

- **Participatory Sensing Layer.** The large-scale pervasive sensing layer involves the three major information sources: mobile and wearable devices, static sensing infrastructure, social web and communication services (cellular or Internet). It utilizes *ubiquitous data capture* as a means to gather knowledge from people nearly everywhere in the world.
- **Privacy Layer.** As privacy and security are major concerns for both private and organizational data, this layer addresses the need for individuals to control access to the data streams to be shared through *personal data vaults*.
- **Leveraged Data Processing Layer.** This layer applies diverse machine learning and data mining techniques in order to infer complex phenomena about individuals and groups from a simple set of collected data.
- **Fusion Semantic Layer.** The fusion semantic layer is used when different features or context need to be aggregated using logic-based inferences.
- **Application Layer.** The application layer includes a variety of potential services that can be enabled by the availability of people-centric sensing systems.

In general, people-centric sensing gives rise to a host of new applications that can be classified into three main groups: (i) *personal sensing*, those focused on personal monitoring and archiving, (ii) *social sensing*, those where information is shared within social and special interest groups, and (iii) *public sensing*, those where data is shared with everyone for the greater public good. In the next section, we describe how researchers envision the use of people-centric sensing in assistive healthcare applications in order to provide a viable alternative to “traditional” assistive living.

3.2. Healthcare Meets People-Centric Sensing Technology

People-centric sensing applications are mainly driven by the needs to (i) develop better social software to facilitate interaction and communication among groups of people, and (ii) predict the real-time change of the world to benefit human life. One emerging application domain is to use

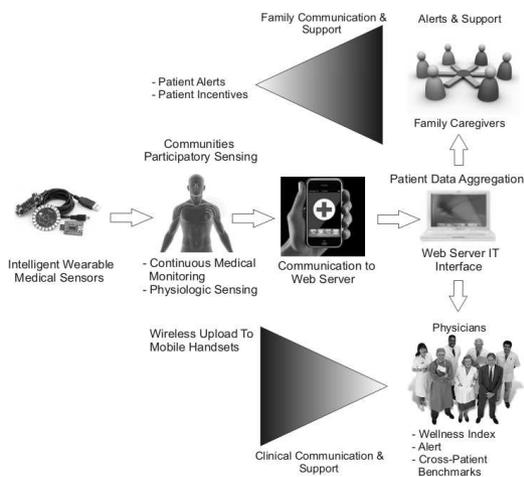


Figure 3. Participatory Sensing as a platform for assistive healthcare support

it as a tool for healthcare and wellness (Figure 3). For example, individuals can monitor themselves to observe and adjust their medication, physical activity, nutrition, and interactions. Communities and health professionals can also use participatory approaches to better understand the development and effective treatment of diseases.

Another possibility for people-centric sensing exists in campaigns for public health: Individuals, healthcare providers, and community organizations could initiate opt-in activities to evaluate and support individualized and preventative care prescriptions, gather data for analysis of causes of chronic and environmentally-affected health issues, and generally to collect a wide range of high-fidelity health statistics for a population of interest. Autonomously captured and selectively shared activity pattern information could help chronic patients and their doctors link environmental factors with symptoms, while explicit data gathering might include automatic upload of at-home, self-administered diagnostic tests.

Finally, this new sensing paradigm can facilitate the anticipation and tracking of disease outbreaks across populations. For example, Epidemics of seasonal flues are a major public health concern. Its impact can be reduced by early detection of the disease activity [6]. Also, healthcare providers can log the physical activities of an individual, track her food intake or sense her mental status in real-time, and record the social activities she attends each day, which can be used to improve human well-being management.

4. URBAN-SENSING PRIVACY CHALLENGES AND DIRECTIONS

Applications that facilitate this new people-centric sensing paradigm, entail serious security and privacy risks. Most of the times, the network infrastructure used in such

scenarios is not owned or operated by any one party, and usually not by the individuals who own the mobile devices used as sensor nodes. The data consumers cannot trust other participants, and similarly, these people will not necessarily trust the system that collects the data or the applications that use the data. Thus, the trust models required are far more complex than those considered in typical sensor-network literature.

Perhaps the most obvious concern is the security of the sensed data itself, especially in correlation to the owner of the device. Unrestricted dissemination of users' sensor data results in breaches of *privacy*; users will want to control who may access information about themselves. Can a participant trust the systems not to track their location? Similarly, can she have access to the sensing tasks they execute or the reports they submit? A balance must be found between giving incentives to users to volunteer their device for data collection and assuring their privacy and anonymity.

Also, since data originates from sensors that are under the control of other people, the *integrity* of the data comes into question. For example, a user may tamper with a sensor device to cause it to report false data, or misrepresent the location or time the data was sensed. Is it possible to operate an open, cooperative network of human-carried mobile handsets when some of the people cannot be trusted to communicate sensor data accurately and quickly?

Finally, a third concern is the *availability* of the infrastructure which is critical for the viability of people-centric sensing applications. Unlike "traditional" assistive healthcare systems where any used hardware and communications infrastructure originate from the same provider, urban-sensing environments assume the involvement of multiple resource providers and administrating organizations. Thus, it is crucial to convince the user of the ubiquity of the technology used.

In the following sections, we detail all the challenges posed towards a secure and trustworthy people-centric sensing system based on the privacy expectations and the concerns of the users themselves. Then, we outline the latest research directions in security and privacy protection that try to deal with all these challenges.

4.1. Privacy and Trust Issues

People-centric sensing faces barriers to wide scale adoption unless users trust the system to provide privacy guarantees. The confidentiality of sensed data goes far beyond the provision of a secure channel from the sensor node to some gateway, as it is the case in traditional healthcare support systems. Such encryption and key-distribution techniques have already been well-discussed in sensor-network security literature. Here, the focus is more on the privacy challenges associated with the collection and dissemination of sensor data.

Compared with personal data (e.g., user profile, medical data), data gathered in communities can reveal much

more information about individuals' behaviors. Privacy decisions have many components, including identity (Who is asking for the data?), granularity (How much does the data reveal about me?), and time (How long will the data be retained?) [43, 44]. For example, an individual's location might reveal his/her interests; collecting health data by communities might have significant consequences on social behaviors towards citizens with diseases. The impact is obvious: if personal data cannot be anonymous and under the control of data owners, people may be less likely to share their data.

Furthermore, people-centric sensing applications in assistive healthcare environments, usually, involve multiple types of context; who should get access to health-related information, who should know whether they are visiting a doctor, and so on. Unlike "traditional" healthcare systems where several systems have been proposed to address specific types of sensor data (e.g., location privacy [45] and privacy of medical data from body sensors [46]), usable mechanisms to protect the *context privacy* of more general types of data have been lacking. For example, an adversary may be able to infer restricted context information from other available data. Care must be taken, therefore, to ensure that context is not inadvertently leaked and that users are tasked and questioned anonymously.

In general, there is a need for discussion about *when* and *how* to share this new form of personal data. Currently, corporations such as mobile carriers as well as small-scale application developers are struggling with how best to provide privacy and confidentiality protections for participatory sensing data. There are three main research areas that deal with these needs [47, 48]:

(1) *Data anonymization techniques*. This class [9, 49] includes all solutions based on the notion of anonymity, which is aimed at making an individual not identifiable when contributing his/her data. For example, *anonymous tasking* and *anonymous data reporting* are being adopted in order for the users to be able to notify the system of their acceptance (of a specific task) without actually revealing their identity. If this is true, the users can share their information without the system knowing their current location. Early solutions involved attribute-based authentication, which ensures that users can authenticate themselves by revealing only a portion of their attributes and not their identities. Another solution suggested the use of static pseudonymous IDs, but soon it was realized that it might be trivial to infer the true identity behind each pseudonym, by linking all user entries together. In general, methods in this class do not guarantee that the process of linking a task or information to an individual is impossible, but that it requires a large effort.

(2) *Enhancing user control and decision making*. User control is very important in personal data sharing as it is about what one wants to reveal and to whom. For example, individuals might want to track their heart rate, but there is no reason to share this information with anyone but their

doctor. Possible solutions to this, are: (i) *selective sharing* by limiting distribution to communities, or perhaps to only a few designated individuals, (ii) *selective retention* by indicating internal dates for personal data collection, thus enabling automatic deletion of information after a specific period, and (iii) *negotiation* with outside parties of the policies and regulations for using and sharing any sensed information.

(3) *Participatory design*. Participatory design (PD) [50] is a practice that incorporates users as co-designers of a system. It involves them in all phases of building a system that fit communities' needs. As we mentioned earlier, people's willingness to share their personal data is variable and highly contextual; thus, system privacy design must respect this variability. PD methods can encourage the participants towards understanding and consensus on system defaults and user choices for data granularity, data sharing, lengths of time for data retention, and reuse policies.

4.2. Integrity Issues

In addition to all the above described privacy issues, integrity of the data sources is another important issue. Most of the times, in urban-sensing communities there is the need to import data from many anonymous participants. In that case, however, is difficult to ensure the integrity of shared information. If a user misbehaves by crafting the data, he/she cannot be blocked from further reporting if full anonymity is allowed. Therefore, data integrity is a conundrum for experts since its quest contradicts the requirements of privacy. Finding a balance between these two settings is a major challenge in urban-sensing environments.

The difference with "traditional" assistive healthcare systems lies in the fact that the adversary is no longer only a malicious outsider compromising a subset of sensor nodes. Here, the threat model includes all the participants that carry a configured mobile handset. Because users are in control of their own devices, they can easily launch attacks targeting the *reliability of shared data*. Furthermore, in the case of healthcare applications, the personal nature of information significantly increases the interest in doing so which, in turn, introduces the problem of *data authentication*; How can sensed data be delivered with the assurance that no intermediate users have tampered with it especially in cases where data must be paired with the producer's identity? For example, if an individual wants to report his/her health-related data to a physician, how can the system ensure the identity of the node to its custodian?

One promising solution area to these needs is to use sophisticated notions for user identity, group membership, and other attributes. For instance, *group signatures* can be employed in order to anonymously verify the validity of mobile sensing devices. One problem, however, with these designs arises from the fact that anonymity can be revoked from group managers or provider entities.

This may discourage attackers, but on the other hand, the revocation capability can be used as a means to track the action of legitimate users.

Another suggested solution includes developing efficient verification protocols that ensure data management and guarantee system and data integrity. For example, a third trusted party could maintain some secure cryptographic state of the entire system configuration, consisting of various user-related parameters. This cryptographic state could be updated and used for verification as network nodes execute queries, tasking commands, and other operations. Such a solution is viable if a trusted entity can be found and there is a balance between the simplicity of verification and the flexibility in securely describing the network state.

4.3. Availability Issues

As we described in Section 2.3, researchers have addressed most of the denial of service (DoS and DDoS) issues for "traditional" healthcare systems. People-centric sensing, however, introduces different kind of availability challenges even though sensed data are submitted by nodes volunteered by their owners. Participants may configure their mobile phones to refuse to accept certain tasks or accept them and then ignore them. This can have severe consequences on the effectiveness of an application as it may depend on the sensing coverage and density. Thus, success of urban-sensing systems is related to the willingness of individuals to participate. This problem becomes worse if we take into consideration the privacy and trust concerns of the users. Therefore, it is crucial to create the appropriate incentives for people to *participate* in urban-sensing scenarios.

One promising direction towards this end is to create applications that fit users needs and have services with clear direct and indirect benefits. This will trigger the communities to experience this new technology by making their mobile devices available for sensing. However, attention must be given to the *fairness* of benefits towards the participants. A balance must be attained in order not to motivate users to cheat trying to obtain better services for themselves than they deserve. For example, in healthcare applications, individuals may task many other sensors to collect information for their own needs (e.g., environmental monitoring of a specific area for levels of moisture, humidity, and other attributes that burden the health of an elderly), without being willing to take on tasks for other users. Research on game-theory principles and reputation-based algorithms could provide useful insights here. In general, the more data-secure, user-private and beneficial a people-centric sensing system is, the more individuals are likely to participate to its services.

4.4. Policy Issues

Software and hardware mechanisms cannot be the sole answer to all the above privacy, security and ethical issues in people-centric sensing applications. Effective trust

regulations must be created that combine technological approaches with institutional policies to enable and enforce protective actions. Policy refers to guidelines or regulations that encourage user engagement and protect participants' data reports. It is an important research direction as it can involve community groups to work through conflicts and make decisions regarding the way sensed data will be used. Therefore, urban-sensing technologies must support both research processes and resulting policies.

Responsibility, however, for all policy settings must be shared between providers (or organizations) and users. It is crucial to include participants to work alongside designers in order to write and enforce system guidelines. Since users are the target group of people-centric sensing applications, it makes complete sense to give them the ability to influence internal compliance policies. Overall, the goal is to come up with a set of policies that complement technology designs and individual participant decisions in order to create an urban-sensing environment where privacy and trust regulations are an important component of any system interaction.

Synergy between policies and technologies entails all of the challenges of interdisciplinary cooperation. The most important, however, is to determine which issues are best addressed by policy or technology. It is obvious that this depends on the kind of application, the participatory sensing domain and the targeted group of users. For example, public health campaigns could require policies for protecting medical records and specific technological approaches for fully managing the collection, storage, sharing, and retention of any health-related data. Furthermore, another question that needs to be addressed is which policy language can be used in order to express users preferences in a readable format even in complex environments? One possible solution is to develop new policy-specification approaches that provide users more extensive settings to accurately specify their regulations keeping in mind not to significantly increase the user burden.

All these issues are still in research as they depend on the context and, therefore, they have to be addressed system by system, domain by domain. However, an attempt is being made to identify those design principles for privacy by policies that are *common* in different community-based urban-sensing systems. This will help the design of future systems in order to encourage people participation by minimizing the risk of undesired disclosures.

5. CONCLUSIONS

Technology advances in sensing, microelectronics and their integration into everyday consumer devices lays the groundwork for the rise of people-centric sensing. With multiple data capturing, positioning, and connectivity

devices, the basic components of a widespread participatory sensor network already exist. There is an exciting challenge to leverage the investment in wireless research and infrastructure to generate a proportional civic benefit. One area in which we see such promise is in assistive healthcare environments as described above.

Effective people-centric sensing will require more than ubiquitous mobile phones and "mass-attractive" services. Such applications have clear and substantial security and privacy challenges, which must be resolved if these systems have any hope of realizing their full potential. Is sensing data with always-on mobile phones a new opportunity to promote healthcare research or is it a very powerful surveillance tool that we carry around in our everyday lives? To answer this question, we described what we believe to be the new challenges in the area, discussed the latest advances, and offered some promising conceptual solution approaches for each. We hope that this paper will trigger a discussion around these issues and better highlight the need for privacy and trust in people-centric sensing applications.

6. ACKNOWLEDGEMENTS

The research leading to these results has received funding from the European Community's 7th Framework Programme (*FP7/2007 – 2013*), Call reference *SEC – 2007 – 1*, under Grant agreement no: 217925.

REFERENCES

1. Chakravorty R. A programmable service architecture for mobile medical care. *Pervasive Computing and Communications Workshops, IEEE International Conference on 2006*; 0:532–536, doi:<http://doi.ieeecomputersociety.org/10.1109/PERCOMW.2006.11>.
2. Shnyder V, Chen Br, Lorincz K, Jones TRFF, Welsh M. Sensor networks for medical care. *Proceedings of the 3rd international conference on Embedded networked sensor systems, SenSys '05*, ACM: New York, NY, USA, 2005; 314–314, doi:<http://doi.acm.org/10.1145/1098918.1098979>.
3. Milenković A, Otto C, Jovanov E. Wireless sensor networks for personal health monitoring: Issues and an implementation. *Comput. Commun.* August 2006; 29:2521–2533, doi:10.1016/j.comcom.2006.02.011.
4. Oliver N, Flores-Mangas F. Healthgear: A real-time wearable system for monitoring and analyzing physiological signals. *BSN*, 2006; 61–64.
5. Chen G, Govindaswamy P, Li N, Wang J. Continuous camera-based monitoring for assistive environments. *Proceedings of the 1st international conference on PErvasive Technologies Related to Assistive Environments, PETRA '08*, ACM: New York, NY,

- USA, 2008; 31:1–31:8, doi:<http://doi.acm.org/10.1145/1389586.1389623>.
6. Milne G, Kelso J, Kelly H. Strategies for mitigating an influenza pandemic with pre-pandemic H5N1 vaccines. *Journal of The Royal Society Interface* September 2009; doi:10.1098/rsif.2009.0312.
 7. Fujiki Y, Kazakos K, Puri C, Buddharaju P, Pavlidis I, Levine J. Neat-o-games: blending physical activity and fun in the daily routine. *Comput. Entertain.* July 2008; 6:21:1–21:22, doi:<http://doi.acm.org/10.1145/1371216.1371224>.
 8. Chiu MC, Chang SP, Chang YC, Chu HH, Chen CCH, Hsiao FH, Ko JC. Playful bottle: a mobile social persuasion system to motivate healthy water intake. *Proceedings of the 11th international conference on Ubiquitous computing, UbiComp '09*, ACM: New York, NY, USA, 2009; 185–194, doi: <http://doi.acm.org/10.1145/1620545.1620574>.
 9. Campbell AT, Eisenman SB, Lane ND, Miluzzo E, Peterson RA, Lu H, Zheng X, Musolesi M, Fodor K, Ahn GS. The rise of people-centric sensing. *IEEE Internet Computing* July 2008; 12:12–21, doi:10.1109/MIC.2008.90.
 10. Eisenman SB, Lane ND, Miluzzo E, Peterson RA, Ahn GS, Campbell AT. MetroSense Project: People-Centric Sensing at Scale. *World-Sensor-Web at SenSys* October 2006; .
 11. Burke J, Estrin D, Hansen M, Parker A, Ramanathan N, Reddy S, Srivastava MB. Participatory sensing. In: *Workshop on World-Sensor-Web (WSW06): Mobile Device Centric Sensor Networks and Applications*, 2006; 117–134.
 12. Eagle N, (Sandy) Pentland A. Reality mining: sensing complex social systems. *Personal Ubiquitous Comput.* March 2006; 10:255–268, doi:<http://dx.doi.org/10.1007/s00779-005-0046-3>.
 13. Wood AD, Stankovic JA, Virone G, Selavo L, He Z, Cao Q, Doan T, Wu Y, Fang L, Stoleru R. Context-aware wireless sensor networks for assisted living and residential monitoring. *IEEE Network* 2008; 22(4):26–33.
 14. J Chen DCJL K Kwong, Bajcsy R. Wearable sensors for reliable fall detection. In *IEEE Eng. in Med. and Bio.*, 2005; 3551–3554.
 15. Sixsmith A, Johnson N. A Smart Sensor to Detect the Falls of the Elderly. *IEEE Pervasive Computing* 2004; 3(2):42–47, doi: <http://doi.ieeecomputersociety.org/10.1109/MPRV.2004.1316817>.
 16. Pappas I, Keller T, Mangold S, Popovic M, Dietz V, Morari M. A reliable gyroscope-based gait-phase detection sensor embedded in a shoe insole. *IEEE Sensors* April 2004; 4(2):268–274.
 17. Moron MJ, Casilari E, Luque R, Gazquez JA. A wireless monitoring system for pulse-oximetry sensors. *Proceedings of the 2005 Systems Communications*, IEEE Computer Society: Washington, DC, USA, 2005; 79–84, doi:10.1109/ICW.2005.20.
 18. Heilman KJ, Porges SW. Accuracy of the lifeshirt (vivometrics) in the detection of cardiac rhythms. *Biol Psychol* 2007; 75(3):300–305.
 19. Liden CB, Wolowicz M, Stivorac J, Teller A, Kasabach C, Vishnubhatla S, Pelletier R, Farrington J, Boehmke S. Characterization and Implications of the Sensors Incorporated into the SenseWear armband for Energy Expenditure and Activity Detection. *Technical Report*, BodyMedia White Paper.
 20. Anliker U, Ward JA, Lukowicz P, Tröster G, Dolveck F, Baer M, Keita F, Schenker EB, Catarsi F, Coluccini L, *et al.*. Amon: a wearable multiparameter medical monitoring and alert system. *IEEE Transactions on Information Technology in Biomedicine* 2004; 8(4):415–427.
 21. Mundt C, NMontgomery K, Udoh UE, Barker VN, Thonier GC, Tellier AM, Ricks RD, Darling RB, Cagle YD, Cabrol NA, *et al.*. A multiparameter wearable physiological monitoring system for space and terrestrial applications. In *IEEE Transactions on Information Technology in Biomedicine* 2005; 9(3):382–391.
 22. Heracleia assist (2009), Research project towards providing remote medical treatment. *Heracleia Lab, University Texas, Arlington* ; [:http://heracleia.uta.edu/project.html](http://heracleia.uta.edu/project.html).
 23. Assistive monitoring project (2009), Research project towards providing remote medical treatment. *Heracleia Lab, University Texas, Arlington* ; [:http://heracleia.uta.edu/project.html](http://heracleia.uta.edu/project.html).
 24. Zplay: An interactive user interface system for alzheimer's intervention. *Heracleia Lab, University Texas, Arlington* ; [:http://heracleia.uta.edu/project.html](http://heracleia.uta.edu/project.html).
 25. Vassis D, Belsis P, Skourlas C, Pantziou GE. Providing advanced remote medical treatment services through pervasive environments. *Personal and Ubiquitous Computing* 2010; 14(6):563–573.
 26. Skourlas C, Belsis P, Sarinopoulou F, Tsolakidis A, Vassis D, Marinagi C. A wireless distributed framework for supporting assistive learning environments. *Proceedings of the 2nd International Conference on Pervasive Technologies Related to Assistive Environments, PETRA '09*, ACM: New York, NY, USA, 2009; 53:1–53:4.
 27. Pantelopoulos N A Bourbakis. A survey on wearable sensor-based systems for health monitoring and prognosis. In *IEEE Transactions on Systems, Man, and Cybernetics*, 2010; 40(1):1–12.
 28. Dimitriou T, Krontiris I. Security issues in biomedical wireless sensor networks. *Proceedings of the International Symp. on Applied Sciences on Biomedical and Comm. Tech.*, ISABEL '08, Aalborg, Denmark, 2008; 1–5.

29. Meingast M, Roosta T, Sastry SS. Security and privacy issues with health care information technology. *IEEE International Conference of the*, 2006.
30. Karlof C, Sastry N, Wagner D. TinySec: a link layer security architecture for wireless sensor networks. *SensSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems*, ACM Press: New York, NY, USA, 2004; 162–175, doi:10.1145/1031495.1031515.
31. Soroush H, Salajegheh M, Dimitriou T. Providing transparent security services to sensor networks. *ICC*, 2007; 3431–3436.
32. Krontiris I, Benenson Z, Giannetsos T, Freiling FC, Dimitriou T. Cooperative intrusion detection in wireless sensor networks. *EWSN*, 2009; 263–278.
33. Krontiris I, Giannetsos T, Dimitriou T. Lidea: a distributed lightweight intrusion detection architecture for sensor networks. *Proceedings of the 4th international conference on Security and privacy in communication networks*, SecureComm '08, ACM: New York, NY, USA, 2008; 20:1–20:10, doi:http://doi.acm.org/10.1145/1460877.1460903.
34. Giani A, Roosta, T, Sastry S. Integrity checker for wireless sensor networks in health care applications. *Proceedings of the 2nd International Conference on Pervasive Computing Tech. for Healthcare*, 2008; 135–138.
35. H S Ng MLS, Tan CM. Security issues of wireless sensor networks in healthcare applications. *BT Technology Journal*, 2006; **24**(2):138–144.
36. Karlof C, Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures. *Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on*, 2003; 113–127, doi:10.1109/SNPA.2003.1203362.
37. Deng J, Han R, Mishra S. A performance evaluation of intrusion-tolerant routing in wireless sensor networks. *Proceedings of the 2nd international conference on Information processing in sensor networks*, IPSN'03, Springer-Verlag: Berlin, Heidelberg, 2003; 349–364.
38. Dimitriou T, Krontiris I. Secure in-network processing in sensor networks. in *Proceedings of First Workshop on Broadband Advanced Sensor Networks (IEEE BASENETS)*, 2004; 384.
39. Chan H, Perrig A, Song D. Secure hierarchical in-network aggregation in sensor networks. *Proceedings of the 13th ACM conference on Computer and communications security*, CCS '06, ACM: New York, NY, USA, 2006; 278–287, doi:http://doi.acm.org/10.1145/1180405.1180440.
40. Tang KP, Keyani P, Fogarty J, Hong JI. Putting people in their place: an anonymous and privacy-sensitive approach to collecting sensed data in location-based applications. *Proceedings of the SIGCHI conference on Human Factors in computing systems*, CHI '06, ACM: New York, NY, USA, 2006; 93–102, doi:http://doi.acm.org/10.1145/1124772.1124788.
41. Floréen P, Krüger A, Spasojevic M (eds.). *Pervasive Computing, 8th International Conference, Pervasive 2010, Helsinki, Finland, May 17-20, 2010. Proceedings, Lecture Notes in Computer Science*, vol. 6030, Springer, 2010.
42. Zhang D, Guo B, Li B, Yu Z. Extracting social and community intelligence from digital footprints: An emerging research area. *UIC*, 2010; 4–18.
43. Kang J. Information privacy in cyberspace transactions. *Stanford Law Review* 1998; **50**:1193.
44. Nissenbaum H. Privacy in context: Technology, policy, and the integrity of social life. *Stanford Law Books*, Stanford, CA, 2009.
45. Gedik B, Liu L. Location Privacy in Mobile Systems: A Personalized Anonymization Model. *25th IEEE International Conference on Distributed Computing Systems (ICDCS'05)*, IEEE, 2005; 620–629, doi:10.1109/ICDCS.2005.48.
46. Tan CC, Wang H, Zhong S, Li Q. Body sensor network security: an identity-based cryptography approach. *WiSec '08: Proceedings of the first ACM conference on Wireless network security*, ACM: New York, NY, USA, 2008; 148–153, doi:10.1145/1352533.1352557.
47. Kapadia A, Kotz D, Triandopoulos N. Opportunistic Sensing: Security Challenges for the New Paradigm. *The First International Conference on COMMunication Systems and NETWORKS (COMSNETS)*, 2009, doi:10.1109/COMSNETS.2009.4808850.
48. Krontiris I, Freiling F, Dimitriou T. Location privacy in urban sensing networks: research challenges and directions. *IEEE Wireless Communications* October 2010; **17**(5):30–35, doi:10.1109/MWC.2010.5601955.
49. Mitchell T. Mining our Reality. *Science* 326 (5960), 2009; 1644–1645.
50. Shilton K, Ramanathan N, Reddy S, Samanta V, Burke J, Estrin D, Hansen MH, Srivastava MB. Participatory design of sensing networks: strengths and challenges. *PDC*, 2008; 282–285.