THE UNIVERSITY OF MELBOURNE

IBES
Institute for a
Broadband-Enabled Society

Participatory Sensing

Enabling interactive local governance through citizen engagement

www.broadband.unimelb.edu.au

November 2014

Authors

Slaven Marusic*, Jayavardhana Gubbi*, Helen Sullivan#, Yee Wei Law* and M. Palaniswami*

*Department of Electrical and Electronic Engineering, The University of Melbourne

#School of Government, The University of Melbourne

Acknowledgements

The authors would like to acknowledge the support of the Institute for a Broadband-Enabled Society, and the input of research students Aravinda Rao and Fu-Chun Hsu. The authors would also like to thank those who contributed domain expertise into the research, particularly representatives from the City of Melbourne, who from across various departments provided valuable discussions and insights into City operations, policies and perspectives. This local insight, complemented by international perspectives obtained through EU FP7 IERC engagement, helped to establish the scale of the challenges and scope of the proposed solution framework.

Extracts from this work have been published in the following article: S. Marusic, J. Gubbi, H. Sullivan, Y. W. Law and M. Palaniswami, "Participatory Sensing, Privacy, and Trust Management for Interactive Local Government," IEEE Technology and Society Magazine, Vol. 33 , No. 3, pp. 62-70, 2014

Further Information

Slaven Marusic: slaven@unimelb.edu.au

Institute for a Broadband-Enabled Society
Level 4, Building 193
The University of Melbourne, Victoria 3010, Australia

ISBN 978 0 7340 4904 9

Executive Summary

Local government (such as the City of Melbourne) is accountable and responsible for establishment, execution and oversight of strategic objectives and resource management in the metropolis. Faced with a rising population, Council has in place a number of strategic plans to ensure it is able to deliver services that maintain (and ideally improve) the quality of life for its citizens (including residents, workers and visitors). This work explores participatory sensing (PS) and issues associated with governance in the light of new information gathering capabilities that directly engage citizens in collecting data and providing contextual insight that has the potential to greatly enhance Council operations in managing these environments.

This white paper examines:

- Key hurdles affecting the viability and uptake of PS from different stakeholder perspectives
- The capacity of PS as a new and mutually beneficial communication link between citizens and government; the respective value propositions in participating, whilst simultaneously increasing engagement and enhancing City operations through co-production with citizens
- Technological elements of PS and associated privacy impacts through the application lens of noise monitoring
- Social impacts of emerging pervasive technologies, particularly the encroachment upon privacy, associated risks and implications, not only for the individual but also the impact in shared environments
- Responsibilities and avenues for mitigation assigned to respective stakeholders; including user awareness factors, policy frameworks and design level strategies
- The role of reputation and trust management between stakeholders in fostering productive links, along with the capacity for citizen empowerment
- The balance of perceived competing objectives of privacy and transparency, ethical strategies to address this challenge
- User perceptions of related issues taken from studies of internet and social media usage through computing and mobile platforms
- A development platform to measure user awareness of privacy risks, behavioural responses to a spectrum of engagement options effectively returning to the user a level of control over their participation
- Essential requirements for responsible implementation of PS platforms, considering ethical issues, responsibilities, privacy, transparency and accessibility

Key findings

Participatory sensing

- The active role of the user is critical for the success of PS, requiring effective engagement, but also mitigation of disincentives, such as privacy concerns. As privacy risks increase in the context of multiplied information sources, despite available privacy preservation strategies, user awareness and control remain key elements.
- Establishment and management of mutual trust is key to PS functioning as an effective medium for communication between stakeholders and for ensuring accountability.
- Citizen empowerment is only achieved with the provision of information to assist individual decision-making, as well as the opportunity for responsibility and control over level of participation.
- Incentivisation schemes need to recognise the value of the data/service being supplied by the user, the accessibility of the organiser provided service and ongoing value propositions

Noise monitoring

- Noise management is essential to prevent adverse health impacts and preserve quality of life. Smartphones can provide indicative measures of noise, but require calibration strategies for the data to be usable. Also, data quality remains greatly affected by user performance.
- Data collection (sound, location) and handling (mobile device and associated cloud services) must reflect privacy principles. Whilst, early deployments have respectively demonstrated selected capabilities, a comprehensive and flexible system catering to diverse needs and perceptions is still required.

Privacy vs transparency

- Privacy is one's control over access and flow of their information. Legal protections are limited to specific circumstances, so ethical means for supplementary privacy protection offer transparency with respect to data accuracy and embed privacy in the design. System transparency and verifiable privacy measures can build trust between stakeholders.
- Social implications warrant mechanisms for managing data history. Additionally, informed user consent needs to be the goal and supported by effective communication of risks. Accordingly, users will utilise various means for protecting privacy, according to their level of awareness and evaluation of risks

Policy frameworks

- Systems for protection of personal information are essential for maintaining/building trust between organisations and citizens. This includes discovery of breaches and recourse for compensation. Existing policies cover data collection and handling; citizen engagement strategies; and feedback management. They reflect privacy concerns; principles of open and responsive government; and value in citizen contributions to governance.
- Limitations of privacy legislation demands supplementary principles/guidelines for system implementation, including industry self-regulation, privacy by design and privacy impact assessment (PIA). Existing and supplementary measures thus need to be utilised and adapted for effective PS.

Pilot study

- The pilot study is based on a noise measurement app and central server for data aggregation and display. The app provides a spectrum of privacy level options, to be selected by the user, that reflect the type and amount of data to be collected/shared.
- The privacy level selection interface serves to inform the user of data handling (and implies associated risk), while a refined interface can more explicitly convey this. This capability demonstrates a means for increasing user control over their level of participation.
- A larger study can expand this capability; provide detailed assessment of public participation capacity; conduct a PIA; reach broader demographics; and further evaluate the issues raised throughout this paper.

Recommendations

- Prior to embarking on PS implementations, organisations thoroughly analyse all stakeholder concerns and ensure necessary steps are taken to address these, as outlined here
- The City of Melbourne look for opportunities to test participatory sensing as a means of addressing specific community concerns in relation to noise nuisance
- Policy makers review existing policy frameworks to ensure that they offer the appropriate combination of incentives and safeguards to facilitate greater citizen involvement in addressing issues of community concern (co-production)
- Policy makers review existing organisational structures and professional cultures to identify any additional barriers to effective citizen engagement

Contents

1 Introduction

Citizen science is the practice of engaging the public to actively participate in research programs through the collection or provision of related data. Tasks may extend to annotating data or providing contextual information not present in the collected data. In this way, citizens are able to contribute not only data collection services, but also essential insights in scenarios where the participant also becomes a subject of the research. Relying on members of the public for data collection, rather than trained personnel, inherently sacrifices some level of data quality. Participatory sensing (PS) as a dimension of citizen science may provide some measure of data quality assurance through the introduction of emerging technologies that assist in sensing, aggregation and validation of data, as well as recruitment and evaluation of participants.

The rapid evolution of information and communication technologies (ICT) in the form of computing and communications devices, together with sensing and monitoring capabilities means that ubiquitous sensing now cuts across many areas of modern day living and offers the ability to measure, infer and understand environmental indicators, from delicate ecologies and natural resources to urban environments. In 2011, the world population of 7 billion was matched by 13 billion connected devices and is expected to reach 24 billion devices by 2020 (according to a study by GSMA and Machina Research). Nowhere is this more evident than in the widespread adoption of smartphones. Fitted with microphone, camera, accelerometer, proximity sensor, GPS, as well as communications via GSM, GPRS, Wi-Fi and Bluetooth that enable additional localisation capabilities, smartphones effectively function as mobile sensing platforms. Additional sensor types can also be interfaced with the phone to provide a greater range of sensing capabilities. For most users, phones are taken almost everywhere and nearly always on, with a variety of sensors active. This presents unprecedented reach into everyday environments that can offer completely new insights into the way people go about their daily lives, how they interact with their environment and with each other.

The proliferation of these ICT devices in a communicating-actuating network creates the Internet of Things (IoT), wherein, sensors and actuators blend seamlessly with the environment around us, and the information is shared across platforms in order to develop a common operating picture (Gubbi, Buyya, et al. 2013). The interpretation of events and visualisation of information for end-users has the potential to enable higher quality of life in the urban environment, through the delivery of smart new ways of urban monitoring using ubiquitous sensing and data analysis for city management and sustainability. This is a key element in the Smart City vision, which proposes the novel utilisation of such emerging and pervasive ICT deployments to address numerous urban living challenges that are becoming increasingly strained. These challenges extend to: urban transport (where impacts of traffic congestion are measured both economically and environmentally); energy and resource consumption (including the delivery and usage of electricity, gas and water services); health and quality of life (including environmental factors, access to services and resources, and mobility).

Population growth in urban centres demands appropriate strategic planning in order to produce a sustainable urban environment with preservation and even an increase in the associated quality of life. Demands on the management of urban environments are made more complex with projected population increases and concentrations of the population in cities and surrounding regions. The City of Melbourne strategic planning initiatives, including Future Melbourne, seek to address these challenges in catering for the needs of its ever-growing numbers of workers, visitors, residents and students, whilst continuing to be an attractive destination for these varied demographics. In-depth sensing, analysis and visualisation of environmental data enables the transition of sensor data, to information and ultimately knowledge, is thus of significant value to City officials. How then is the City able to access this highly valued data? If this information transfer is reliant not only on newly emerging sensing and data collection capabilities, but also on the willing contribution of such data by citizens, then how is this best achieved? Similarly, citizens may also find benefit from directly accessing such information. In this way, such platforms whilst serving multiple stakeholders may also provide a new mechanism for exchange of information between them.

1.1 Citizen Engagement

Citizen engagement in public policy making and delivery occurs in a variety of ways and for a variety of purposes (Barnes, Newman and Sullivan 2007). In democratic societies, citizen engagement is promoted as a way of enhancing the quality of democracy by improving trust relationships through closer and more responsive interactions between decision makers and citizens. Increased citizen participation is also promoted as a way of securing improvements to quality of life for current and future generations by drawing on citizens' lived experiences to inform public policy making and service delivery. Governments often explore citizen engagement techniques with excluded or marginalised communities in order to access better information about community needs, build relationships and design more appropriate policies and services. Current debates focus on citizens as 'co-producers' of public policy and public services, their contributions providing vital resources to complement the work of professionals (Ostrom 1999).

A recent analysis of urban health by the City of Melbourne has revealed ongoing challenges around social inclusion, noting that 46% of citizens participated in engagement activities (below the Victorian average of 53%), with only 41% providing input into associated issues (compared with the Victorian average of 45%) (CoM, Urban Health Profile 2012). The degree of desired public participation may also vary according to the needs of government in addressing a given issue. This can span direct involvement in the decision-making process, to the policy or engagement platform design; or be restricted to consultation to gauge citizen views or market test ideas (Evans and Reid 2013). A technology platform that implicitly involves citizens in local government issues can help to address the challenge of improving citizen engagement (through increased participation and meaningful interaction) providing the right incentives and protections are in place.

Technology can assist in filtering vast volumes of information such that it can be meaningfully interpreted by the user; and can simultaneously function to inform and educate (Evans and Reid 2013). However increased technological capability comes with attendant risks, in this case how user privacy is protected and informed consent obtained.

The manner in which such technological capabilities are developed and deployed has a significant bearing on determining the subsequent beneficiaries and to what degree they draw any benefits. More specifically, which stakeholders are able to benefit from this emerging technological capability and indeed, can the development be framed in a manner that allows diverse stakeholders to simultaneously benefit? This work takes the issue of noise management as a case study to explore whether emerging IoT technology in the form of smartphones and associated cloud computing services can be effectively utilised for participatory sensing in a manner that enables greater citizen engagement and involvement in local government processes.

1.2 Noise

Considering health and quality of life in the urban environment, noise pollution and its management is a critical concern. Extended exposure to excessive noise is known to have negative effects on health, well-being and quality of life, providing a significant challenge to city councils in managing noise and its effects. Currently, city councils (such as the City of Melbourne) rely on public complaints to define the issue of noise rather than the best practice method of noise mapping. This has left a gap in the ability to effectively manage and prevent increases in excessive noise. They presently rely on cost and labour intensive manual measuring, meaning it is only applied to specific areas and on a one-off basis. Incidentally, noise complaints have increased in recent times (from 1149 complaints in 2010-2011, to 1378 in 2011-2012), noting that noise management in an area in need of improvement (CoM, Urban Health Profile 2012). Whilst noise is largely subjective, negative impacts have already been identified. These impacts can be observed independently of the individual's perception of the noise source itself. It also relies on the subjective experience being such that it exceeds the threshold at which the individual is motivated to register the complaint. In this way, the current system has the potential to miss those individuals who are less likely to complain, don't know to whom to complain or are simply prepared to endure the noise (with the continued exposure and health risks).

1.3 Participatory Sensing (PS)

The need for a reliable system for measuring noise, monitoring noise and responding to noise issues is a key driver in the development of wireless sensor network (WSN) systems for urban sensing, forming one element of an urban IoT system. However, fixed sensing infrastructure, particularly in the context of high-density deployments, has substantial cost implications (Palaniswami, et al. 2011). The wide availability of mobile sensors (e.g. smartphones) presents other opportunities for collecting vital environmental information. The proximity of the sensor to the point of interest when considering subjective impact factors such as noise, makes PS an attractive capability (Rana, Chou, et al., Ear-Phone: An End-to-End Participatory Urban Noise Mapping System 2010) (Santini, Ostermaier and Vitaletti 2008) (Maisonneuve, et al. 2009).

In essence, the citizen is participating in the data collection process by sharing data collected from their own device. The functionality of smartphones, as seen with respect to social media, provides a convenient mechanism for sourcing user feedback in addition to raw data collected by the sensors on the device. This becomes highly valuable in adding context to events or measurements observed by the sensing platform. A mobile people-centric sensing platform provides a mechanism for engaging citizens, as well as obtaining valuable feedback and an understanding of the public perceptions of noise and urban sounds. This in turn can help identify local soundscapes and the desirability and usability of urban spaces. Substantial hurdles still exist that potentially affect the viability of this scheme, including factors such as the motivation for citizens to participate, the sparse nature of data collected, data validity and utilisation of user collected data and feedback within government.

Insights to this challenge were formed through initial engagement with Health Services at the City of Melbourne. Subsequent participation in the EUFP7 IoT European Research Cluster and projects SmartSantander and SocIoTal has provided insight across the spectrum of application specific data collection to the utilisation of extracted information by stakeholders. The 2013 meeting of the associated IoT Forum further fostered the questions of data ownership along with responsibility for data management and establishment of associated protocols. Additionally, the 2012 Digital Melbourne workshop conducted by the City of Melbourne considered the importance of citizen engagement through the kind of PS described here. Attended by a cross-section of the community (citizens, tech savvy city users, academics, industry representatives, City administrators), discussions spanned privacy of users, security of data and incentivisation schemes to encourage participation. Proactive incentivisation schemes and associated reward mechanisms need to reflect City viewpoints on accessibility and fairness. Accessibility is similarly reflected in the availability of a variety of interface platforms and how this may affect the sample size and diversity of participants. Finally, privacy being highlighted as a key aspect motivated this exploration of mechanisms to determine privacy concerns and behavioural responses.

1.4 Objectives

The focus of this work is to identify and address the key hurdles affecting the uptake of this capability from both citizen and government perspectives. In doing so it poses key questions that aim to shed light on this objective.

- Is participatory sensing indeed a functional tool for enhancing communication between citizens and government?
- In this way, does it enable interactive local governance, not presently achievable through traditional means?
- Is such a platform able to service the diverse interests of multiple stakeholders?
- What are the essential requirements of these different users?
- What is the significance of incentivisation criteria and the associated capacity to deliver genuine citizen engagement?

In exploring these questions, the work also seeks to identify the significant factors that influence the technological viability of participatory sensing, explored through the context of noise monitoring. It must be noted, that noise monitoring is a representative application, selected as it serves the interests of multiple stakeholders and so can demonstrate the potential for PS to function as a genuine 2-way communication or information-transfer link.

The work is not solely focussed on technological viability, but importantly looks at the social viability or palatability of such emerging technological platforms. As such, it is a window through which to begin assessing the broader implications of PS and eventually IoT. It considers the prospect, through the appropriate combination of technological design, policy framework and balance of incentives and safeguards, of implementing technological solutions at the service of the person. It does this by addressing existing disincentives for participation. The work seeks to highlight the following:

- The role of privacy and its preservation
- Managing trust and reputation between and amongst stakeholders
- Citizen empowerment
- Ethics in platform design and the balance of privacy and transparency
- Essential policy frameworks to deliver necessary accountability

Finally, a development platform is proposed that provides direction for the ultimate deployment of PS in a manner that seeks to balance the interests of these different stakeholders. This platform will incorporate the capacity to actually determine these interests and the significance with which they are held by the various participants. Rather than making assumptions about the perceptions of users with respect to certain functions and vulnerabilities, the proposed platform will determine these implicitly. This step is proposed to accurately determine user preferences and the impact that availability of interaction options have upon user interaction with the platform and ultimately with other stakeholders through the platform.

2 Participatory Sensing

In recent years there has been a very rapid expansion in the number and size of websites devoted to gathering information supplied on a voluntary basis by users. This phenomenon of crowd-sourcing is part of a more general trend of user-generated content facilitated by technologies such as Web 2.0, smartphones and GPS. In the context of geo-spatial systems this is called Volunteered Geographic Information (VGI) that complements the traditional components of spatial information collection by drawing upon the collective observations and expertise of citizens in their everyday lives (Longueville and Smith 2009).

Participatory sensing is the framework for large-scale collection of user supplied sensor data from mobile devices. It offers the possibility of low cost sensing of the environment localised to the user. Also referred to as people centric sensing or crowd sourcing of data, it can therefore give the closest indication of environmental parameters experienced by the user. Importantly, it offers the opportunity for the user to provide feedback on their experience of a given environmental parameter that offers valuable information in the form of context associated with a given event. The people-centric sensing system provides contextual information regarding noise sources, as well as critical input to the soundscape analysis. Additionally, the environmental data collected by users forms a social currency (Kuznetsov and Paulos 2010).

There are a number of stakeholders, which stand to benefit from PS applications, each with different motivations. These include: the system operators or organisers; the participants; and end users of the collected, analysed and displayed data. The organisers deploy the system, aggregate the supplied data and display relevant outcomes, either internally within the host organisation, privately (accessible only to the participants or third parties with a specific interest in the application data) or publicly. In principle, the organisers will maintain access control to the platform; provide necessary security guarantees; and system support. Motivation for such service provision by organisers, may vary from gaining access to new data streams for operational or commercial interests, sourcing user insights into associated issues, or enhance service provision based on new environmental data.

The PS system user (or participant) is responsible for collecting the data utilising the mobile sensing platform. The level of dependency on the user actively sourcing samples is determined by the application needs and the system operation requirements. The system may be set up in manner that requires manual activation and inputs from the user. Alternatively, it may be automated, such that the phone itself detects when sampling is required, activates necessary sensors and then collects, stores and uploads corresponding data to central repositories operated by the organisers – all without requiring any further handling by the user other than the initial activation of the phone's PS application. Participant motivations are varied, from altruistic (providing data for some collective benefit), individualistic (seeking to benefit directly from the information gained from self-collected data or data supplied by others) or both (where users contribute data and equally benefit from the service provided by the PS organisers) in addition to possible financial or service based incentives that may be applied.

2.1 Privacy risk

In literature associated with PS, social media platforms and now IoT, privacy concerns are listed as a significant issue. However, insufficient attention is given to the nature of these concerns, such as: the implications and risk factors of inadequate privacy protection measures; the impact on technology utilisation of users' actual understanding of existing risk factors and any safeguards that may be available. Solutions that are provided are often limited in scope. Indeed, there is a risk that designers will focus on development of new system capabilities, neglecting the necessary ethical dilemmas by associating these challenges with data utilisation and so a task for someone else (Shilton, Participatory Sensing: Building Empowering Surveillance 2010). A survey of PS applications and associated challenges is provided in (Christin, Reinhardt, et al. 2011). Importantly, they acknowledge the lack of flexibility needed to reflect diverse viewpoints and awareness of privacy risk, implications and available mitigation strategies.

The first privacy requirement is the provision of secure communication links between the user and platform (hosted by the service provider). Conventional data encryption methods available on mobile computing platforms (such as Secure Socket Layer (SSL)/Transport Layer Security (TLS)) intend to ensure that only the intended receiver of the data transmissions is able to access the contents (De Cristofaro and Soriente 2013).

One of the obvious risks associated with PS applications is the same as that of any data sharing application, where *the information being shared may actually reveal more about the user than is being intended, or agreed upon*. It is now widely accepted that users of social media platforms need to take care in the way personal information is shared or publicly displayed, particularly when utilising multiple platforms. It has been demonstrated that seemingly innocuous postings can reveal information about location, behaviour, routine, social networks and identity. This may be described as information leakage, where it crosses over to another domain or platform to reveal either something more detailed or completely new when combined with other data. Each of the sensing modalities available on smartphones present the risk of revealing private information, from: daily routine (based on time stamped location); identity (from photos, gait analysis, voice recognition); or associations (from photos and voice recognition).

Sensor	Location	Identity	Activity	Associations
GPS/Wi-Fi/Bluetooth	X		X	
Audio	X	X	X	X
Camera	X	X	X	X
Accelerometer		X	X	

Table 1: Information Leakage

Importantly, the nature of participatory sensing has the capacity to reveal information, not only about the user, but also about others in their vicinity. Therefore, in addition to personal risk of exposure, awareness also needs to be established of the secondary exposure introduced into a given environment. Providing adequate safeguards is thus a multidimensional problem (Christin, Reinhardt, et al. 2011).

When the associated services are primarily location focussed, such information has real-world implications. Location can be established, with varying degrees of accuracy, from GPS signals, cell tower locations, as well as from Wi-Fi and Bluetooth links to associated infrastructure. For example, some traffic authorities have deployed infrastructure to detect Bluetooth devices of vehicle users in order to map vehicle paths and travel times. Whilst in such instances, the information is being utilised to improve traffic flow and road infrastructure services, it demonstrates the vulnerability of individuals in allowing unsecured access to their communications and the secondary information that can be extracted from doing so. These concepts have also been explored in the context of Intelligent Transportation Systems that utilise various means of vehicle identification from license plate recognition, electronic tags for tolling systems or GPS devices. The roles of different interested stakeholders are noted along with the potential for establishing personally identifiable location information and how existing US privacy law impacts such operations (Garry, Douma and Simon 2012). Similar challenges have been faced by location based services on mobile phone or computing platforms for some time (Anderson, Henderson and Kotz 2007) (He, Wu and Khosla 2004) (Shahabi and Khoshgozaran 2007).

2.2 Privacy preservation

There exists a suite of proposed solutions for preserving privacy in participatory sensing whilst still permitting a desired level of engagement in the program, with some taken directly from networked computing strategies.

The first option is to provide some degree of **anonymity** for the user. It must be determined then, from whom anonymity is required, or rather, for the meaningful operation of the PS platform, for whom is identification required/permitted. It is widely acknowledged that users demonstrate different degrees of willingness in sharing data, depending on the relationship with the other party (or parties) involved.

Degrees of identity revelation maybe classed as:

- Completely anonymous
- System Organisers/Network Operators
    - Requires secure end-to-end communications regardless of the number hops or network types utilised in the transmissions (e.g. Tor).
- Selected peers/participants
    - A user/organiser defined subgroup, established based on certain criteria, such as pre-determined trust or existing community group.
- Other participants on the system
    - Identifiable to other users with access rights to the system.
- Anyone able to eavesdrop given communications links somewhere along the network
- Notionally hidden, but unsecured.
- Open

- Unrestricted publishing of identity linked with data contributions

Providing anonymity is not without its own implications. If not carefully designed, a system permitting anonymous contributions can be easily compromised if there is no means of verifying the quality and validity of the data. In such cases, it may leave organisers with no recourse to identify or manage misbehaving or malicious users. In this respect, the same tools that protect the privacy of the innocent also hide the identity of the malicious or criminal.

The common argument that is often posed in shifting the balance of privacy towards transparency is that some privacy must be sacrificed in order to ensure security. If this is indeed true and unavoidable, then certain questions immediately follow: to what degree must privacy be sacrificed; to whom is privacy to be sacrificed; and what level of trust can be assigned to this authority? Indeed, is it even possible to apply a threshold in trying to answer these highly debatable questions? Consideration must be given to the risk and implications associated with any subsequent abuses of this trust. So whilst a goal may be set for balancing privacy and security, according to some established value system, the viability of such thresholds only exist in as much as aggrieved parties have recourse to compensation from any breaches. Where this is implausible to guarantee, a more cautious approach would be to first question whether the emerging capability is actually increasing the degree of vulnerability of users without adequate protection and for insufficient return/reward for their participation.

From a practical perspective, a number of measures can be implemented at the design level, that provide users with varying levels of protection. Some of these include:

- Masking identity (utilising independent verification methods; allowing anonymous data contribution; simulating high participant density)
- Masking location (data perturbation or reduced granularity)
- Limited data release (sharing of aggregated or filtered rather than raw data)

Essentially, such methods rely on the existence or appearance of a large number of users within the system and within the specified location (k-anonymity), so increasing the difficulty with which a single user (or their data) may be identified. In this way, the system can compensate for malicious users (e.g. supplying misleading data); unreliable users (e.g. supplying incorrect/erroneous/low-quality data); collaborating users (e.g. to uncover identity or other restricted information about other participants; bias overall measurements; manipulate user reputations).

Self-surveillance describes the personal information that is captured, stored and potentially transmitted though the complicity of individuals. To combat the increased vulnerability to privacy breaches arising from self-surveillance and indeed the expected decreasing privacy, the concepts of Personal Data Vaults (PDV) and Personal Data Guardians (PDG) have been proposed as a means of giving users greater control over how their data is shared, whilst still making use of cloud infrastructure (Kang, et al. 2012). Self-surveillance applications relate more to measurement of biological parameters, activity and mobility. As such, whilst obviously of interest to the individual, there is also substantial interest from third-parties in being able to analyse and aggregate such data to deliver population-wide insights. There is a need then to balance the usefulness to the individual of such applications, whilst also being able to share some aspects of this data (agreeable to the user) with outside entities. The PDG serves as a trusted entity, with whom the user enters into a legal, fiduciary and confidential relationship (in a similar fashion to that with lawyers or doctors). In proposing PDG to act as trusted intermediaries, the flow of data is slowed, thereby preserving some degree of privacy.

Despite the advantages that PDVs seemingly provide, the privacy guarantee of a system that proposes secure storage in the cloud and transmission utilising many layers of communications infrastructure is difficult to ensure, particularly in light of many well publicised hacking and spying episodes. *Two issues remain unresolved; the first is public perception of the degree of security available, whilst the second considers user behaviour in light of available security of privacy options and concern for associated risks.*

Investigating user perceptions of cloud computing security and data vulnerability in (Ion, et al. 2011), it is observed that a large degree of scepticism still exists impacting what users will store. There is also general acceptance that existing means for presenting Terms of Service (TOS) are largely ineffective, in that they are difficult to understand or generic and thus often ignored. As many as 51% of users don't read online privacy policies, with most perceived as too long or complex and of those who read privacy policies, only 37% are able to gain the necessary information to decide whether or not to use the site (OAIC, Community attitudes to privacy survey 2013). This results in mismatched expectations of users as to their rights and the actual requirements of the service provider. Further complexity is introduced by changes across demographics and culture, in how privacy risk is perceived and trust of organisations assigned (Bélanger and Crossler 2011). Analysis of TOS for cloud services has also revealed a tendency for bias towards more detail regarding user obligations rather than the provider's, with the authors recommending a legal framework (albeit in the US context) offering greater control and portability for the user for the management of their data (Kesan, Hayes and Bashir 2013). Ultimately, the effectiveness of any service guarantee is only as effective as one's ability to detect contravening behaviour and the scope for compensation.

It must be considered whether the majority of users interact with these services naively or well-informed. The significance of such factors is often merely assumed and only interpreted in terms of the effect on the total number of users, following which a range of privacy preservation measures are proposed in order to mitigate any detrimental impact on participation rates. In (De Cristofaro and Soriente 2013), the provision of adequate privacy protection is considered the single most important factor affecting the willingness of users to contribute data. Consequently, they propose a cryptographic system for Privacy-Enhanced Participatory Sensing Infrastructure (PEPSI), based on Identity Based Encryption and third-party generation of decryption keys (private key generator). They also acknowledge challenges in protecting query privacy from organisers; node privacy from network operators; and collusion attacks.

2.3 Reputation and trust

Trust management systems may be categorized as either rule-based or reputation-based (Yang, Zhang and Roe 2012). A rule-based system applies credential matching, based on credentials (certification), chain discovery (with importance placed on associated storage locations) and trust negotiation (protecting credentials, avoiding unnecessary exposure). Reputation-based trust management characterises user behaviour by collecting, distributing and aggregating assessments of user contributions in a way that may identify malicious behaviour. They describe the different stages of trust management as establishment of initial trust; observation of behaviour; and evolution of reputation and trust. Initialisation is always problematic, as there is little on which to base an applied trust level. Approaches have been proposed that draw on community ratings of new participants; however, this does not preclude other participants from providing biased or malicious reports.

The more conservative approach will allocate a low trust level to new users with a period of time for this reputation to be improved. The alternative is to assume trustworthiness and then downgrading the assigned trust level if warranted. In observing behaviour, anomaly detection methods may be applied to automatically detect potential misuse, by first classifying normal behaviour in a way that enables rapid detection of anomalous behaviour.

The impacts of these respective decisions needs to be quantified and related to the number of users in the system in order to determine the effectiveness and suitability of the associated trust management framework. This is particularly important when considering the concept of sharing reputations across communities, reputations on which other communities can then initialise their own trust levels for new users. This reaches back into questions of privacy, with identification being required across different domains. It also draws into question the reliability of trust management frameworks in one domain and their impacts on other domains. This may point to the need for a central trusted authority. Yet a distributed approach, applied with certain safeguards and agreed criteria, provides some protection against attacks on a single central repository of reputations.

Existing reputation models include: summation and average (aggregation of ratings to produce a single reputation score); discrete trust models (assigning labels to actions for ease of interpretability); and Bayesian systems (applying positive or negative ratings along with a probability distribution to determine reputation) (Reddy, Estrin and Srivastava, Pevasive 2010 2010). The first is susceptible to bias if the number rating is heavily skewed towards one side, while discrete models (non-mathematical) do not inherently support statistical inference of reputation confidence. Bayesian systems, however, offer the ability to establish a measure of confidence in the reputation score, by determining the probability that the expectation of a distribution (which determines the reputation) is within a certain error margin. It also allows for weighting of new and old measurements, effectively applying a forgetting factor, to more effectively update reputations giving preference to either more recent or historical behaviour.

Another system evaluates a number of different attributes that are combined to determine reputation (Abdulmonem and Hunter 2010). These include: direct rating between members; inferred trustworthiness; rating of observations; contributor’s role/qualifications; quality of past contributed data; completed training programs; amount of contributed data; frequency of contributions.

In a similar fashion, (Yang, Zhang and Roe 2012) proposed a combination of direct information (objective evaluation based observable parameters), personal information (personal information which infers a degree of accountability if accurately provided) and indirect reputation (subjective measures such as community and organiser's trust). As mentioned earlier, the last criteria is problematic and thus needs to be weighted accordingly, while personal information can similarly be weighted according to the level of detail supplied and its verifiability. In fact, this challenge was reflected in their experiments, observed in a small number of participants not willing to supply personal details.

In (Christin, Roßkopf, et al. 2012), the user reputation is cloaked utilising cryptographic primitives. Similarly based on k-anonymity, in (Huang and Kanhere 2012) a trusted reputation server is utilised in a manner that masks the reputation in transit so as to reduce prospects of linking user identity to reputation by external parties, whilst claiming greater flexibility in reputation assignment and accuracy. In (Wang, et al. 2013) anonymity and reputation challenges are balanced through the separation of the data reporting and reputation update processes.

2.4 Citizen empowerment

The earlier transport example demonstrates an information extraction mentality that can exist amongst service providers. Albeit for enhanced service provision that benefits the consumer, the consumer is still largely considered an information source. A shift in this paradigm, that recognises the value in user engagement, has the potential to open up richer sources of information than what is passively supplied by unknowing targets, whilst encouraging two way information flows for mutual benefit. We see this too in transport networks where live traffic updates can be obtained as well as real-time scheduling of public transport. This can be further enhanced with contextual information supplied by the participant, such as the occupancy level on public transport, or reporting of road hazards. These examples point to the potential of citizens as co-producers of improved services, their provision of experiential knowledge complementing the existing technological infrastructure and professional expertise.

A functional PS platform that is utilised not merely as a means for extracting data, but rather as a tool for informing users of all aspects of their participation, has the potential to transform the way citizens and service providers understand the choices that are available to them and the impact of their choices. Traditionally, this understanding has only been available at the scale of large populations due to the lack of fine-grained monitoring of infrastructure, services and users. The challenge we seek to address, is how to empower stakeholders to make more informed decisions based on the ability to interpret information available from a rich sensing infrastructure. A key element is empowering citizens and service providers to change their behaviour, through better-informed decisions. This can also help service providers understand market segments of users for their services, identifying communities of similar users and how the service provider's policies affect those communities.

Utilising PS as a means of empowering citizens is explored in (Shilton, Participatory Sensing: Building Empowering Surveillance 2010), reflecting the objectives of citizen science and participatory research as a means of engaging groups or communities in issues which they are directly affected. It is differentiated from traditional surveillance by maintaining goals of local control, participation, transparency and social justice, with the latter in particular, setting it apart from social or interpersonal surveillance (Andrejevic 2007). *The empowerment comes as a result of placing the responsibility and* *control of data collection and supply in the hands of the users, giving them direct input into the design, analysis and review of key questions posed in the PS deployment*. In addition, it shifts their role from passive subjects, being monitored and analysed, to active participants. Whilst this does not provide a significant shift in the power balance between citizens, government and corporations, it does at the very least offer citizens a new voice. It also reduces their reliance on external organisations to provide insights regarding their local environment by providing them with tools to perform their own monitoring and analysis.

2.5 Incentivisation

A significant limitation of PS applications reported thus far, has been the challenge in obtaining sufficient volumes of data, both from individual participants as well as attracting a sufficiently large number of participants. Both of these factors greatly influence the usefulness of the collected data across a variety of applications. With a limited population size, the demographic spread of users may be too small to establish sufficiently diverse perspectives from the available data. This is relevant for example, when attempting to map positive or negative perceptions of a given soundscape and so determine which demographics are impacted and how. However, if the objective is merely to collect as many noise level samples as possible to build a noise map, then only the total number of samples collected is of interest, rather than the number or type of people collecting them. That said, more people participating would have additional benefits, such as overcoming any bias in the measurements from a single provider. Such bias is introduced through the inherent variability in the sensing framework. In the case of noise monitoring, this will include sensor variability in the actual built-in microphone from one phone to another (even between the same model). This requires calibration where possible. Further variation is introduced by the users' ability to take quality measurements, requiring consistent sensor placement. For this reason, noise measurements taken by city officials, or contracted experts, are performed according to specific guidelines to ensure that measurements are as consistent as possible, regardless of the person performing the task.

Many assumptions about the extent and duration of user engagement may be made, with a number of these supported by early trials of PS applications. This can be said of interest level as a factor in ongoing engagement, which is expected to peak during the introductory phase, perhaps supported by promotional campaigns. Without subsequent incentives, participation rates drop markedly. This can be mitigated by providing a continuing value proposition to the user. This may be the provision of associated services that make use of participant data.

As PS is fundamentally reliant on active user contributions, the sensor data supplied by users has implicit currency. This can be factored in when considering incentivisation schemes to maintain user interest and subsequently adequate data supply to service the associated application. In (Luo and Tham 2012), this principle is applied in the utilisation of a service quota that is granted to users by the service provider. They apply a fairness principle to ensure that users have adequate access to the service, factoring data contribution, requested access, user cost (battery, network access charges) and their assigned quota. Of course, this is more relevant where service provision is resource constrained. Alternatively, this can be interpreted in terms of a service level that is correlated with the data level contributed. In this manner, they also apply an incentive with a (so called) social welfare maximisation, where users are incentivised to contribute at higher levels, based on a game theoretic approach in order to find the optimal distribution of the utility services.

Whilst for most PS applications it is advantageous to attract as many participants as possible, it has been noted that certain targeted campaigns may benefit from utilising a specific audience. This may be due to the need to more efficiently utilise limited resources or where the input from a selected demographic is desired. Additionally, by attracting the desired audience, the organisers may indeed be able to achieve a more effective and perhaps longer-term engagement in the activity by effectively screening participants.

In (Reddy, Shilton, et al. 2009), a recruitment system is proposed based on user mobility profiles that most closely match the geographical area of interest. In order to protect user privacy during the recruitment phase, only limited information is collected, stored and retained for a fixed period of time. They note as future work, the need to clearly and effectively negotiate with the users the privacy parameters being applied, such that informed decisions are made. Items include knowledge of requester's identity; granularity of the data (level of detail); data usage purpose; and duration of data retention. In subsequent work, graphical tools are proposed to visualise data being released in order to enhance user awareness (Shilton, Burke, et al. 2008).

Of equal importance to the viability of PS is the usefulness to the service provider. In this context, that role is played by local government and the determining factor is how the PS supplied data is to be utilised by the City. This can occur on many levels depending on the quality of data being supplied and operational tasks that are being enabled, aided or enhanced by the provision of the new information stream. The usability of PS data contributions may include assisting officials in enforcing public policy, where PS data serves as supporting evidence, whilst lower quality data may only be useful in an informative context, providing insight into community perceptions and potentially informing City policy or programs. Whilst for this work we consider the potential of PS in noise monitoring to both citizens and government, it is ultimately the transferability to other application domains that will determine how useful PS is and beyond specific applications, its ability to foster improved communication between citizens and government.

2.6 Key points

- **The active role of the user is critical for the success of PS**
- **It requires effective engagement, but also mitigation of disincentives**
- **Privacy risks increase in the context multiplied information sources**
- **Whilst privacy preservation strategies are available, user awareness and control are key elements**
- **Establishment and management of mutual trust is key to PS functioning as an effective medium for communication between stakeholders and for ensuring accountability**
- **Citizen empowerment is only achieved with the provision of information to assist individual decision-making, opportunity for responsibility and control over level of participation**
- **Incentivisation schemes need to recognise the value of the data/service being supplied by the user, the accessibility of the organiser provided service and consider ongoing value propositions**

3 Noise monitoring case studies

Exposure to excessive noise levels is known to negatively affect quality of life. These effects, though largely subjective, can be broadly categorized as annoyance (affective-emotional response), affected concentration, communication disturbance and sleep disruption. While instances of sleep disruption and affected concentration (represented by interruption of an activity in response to a noise occurrence) can be measured, annoyance is determined based on the perception of given sounds or as a consequence of the former effects. Further to this, exposure to excessive noise levels is known to have detrimental health impacts (at sound pressure levels above 65dBA). Some of these effects include (a) stress, anxiety contributing to mental illness; (b) pain (at 120dB); hearing damage (at 85dB); (c) sleep disorders, hypertension; heart diseases (Sobotova, et al. 2010) (Vernez Moudon 2009). A single burst of noise can affect endocrine, neurological and cardiovascular function, while frequent exposure can result in chronic physiological disturbance. Experts estimated 80 million people suffered unacceptable noise levels and 170 million experience serious annoyances during daytime in the EU (Miedema 2007).

A 2007 social survey by Australian state Victoria's Environmental Protection Authority (EPA) found that almost half of the people surveyed (49 per cent) were disturbed or annoyed by environmental noise and one-quarter (24 per cent) of respondents reported sleep disturbance at some stage in the last 12 months. The World Health Organization (WHO) has developed Guidelines for Community Noise (1999) and while mean levels across Melbourne are close to these guidelines, the number of sites exceeding recommended levels is significant (EPA 2007).

3.1 Hardware capability/limitations

A number of smartphone applications have been developed in recent years that utilise the existing microphone to measure noise levels. These different hardware and software platforms respectively demonstrate the potential for utilisation in participatory sensing applications, whilst also identifying various limitations, including: the in-built sensors; the associated phone app; the data storage and processing requirements; upload functionality and data display tools. These vary between application specific limits and more general issues relating to user privacy and data integrity.

The first of these is the reliance on the built-in microphones, tailored for voice communications, rather than wide ranging audio sources. The associated compromise in range and sensitivity limits the performance of the phone as a noise level monitor, differentiating it from commercial handheld noise level monitors used by council officials and associated experts.

The WideNoise iPhone application measures noise levels (in decibels) enabling individuals to gauge the noise level in their immediate environment using their phone, along with the ability to share the information online (Widenoise 2009). Measurements are calibrated using a sound level meter and adjusted to compensate for the physical limitations of iPhone's built-in microphone (which filters the human voice against background noise). While able to provide a useful indicator of the local soundscape, the readings are not accurate enough to be used as dB readings required in high accuracy applications.

Noisetube, similarly utilises mobile phones for noise pollution monitoring, adding functionality for tagging events or readings and sharing this information and creating associated noise maps (Maisonneuve, et al. 2009). In this way, it seeks to address the user experience of noise. It is geared towards empowering citizens to monitor and manage their environments and supporting behavioural change. The algorithm takes 1 second samples from the phone's microphone and determines the sound level in dBA, with measurements either sent to the NoiseTube server in real-time or saved and uploaded later. Location tagging is based on GPS readings. For privacy concerns, no audio recordings are stored. Noted challenges were the engagement of the community in order to obtain sufficient data to create meaningful maps, and in particular, the continued participation beyond short-term campaigns. Technical support only being available for a limited number of high-end phones is also a limitation.

NoiseSPY (Kanjo 2010) is another sound sensing system utilising a mobile phone as a low cost noise data logger. The research concluded that while the functionality of participatory sensing is engaging for users, many aspects such as personalization of data and contextual information are important factors in obtaining and retaining interest. Dual purposes of noise mapping and personal exposure analysis were evaluated. It was noted that while the ubiquity of mobile phones make mass participation feasible, actually motivating a sufficient number of participants remains a challenge. Other issues (common to similar deployments) include: location accuracy, power management, privacy and phone resource demands.

PRISM is a Platform for Remote Sensing using Smartphones (Das, et al. 2010) to aid in the realisation of participatory and opportunistic sensing applications. The platform tries to balance generality, security and scalability, managing un-trusted applications on smartphones by allowing controlled access to in-built sensors and sensitive data. Results were evaluated on a small-scale deployment of Windows Mobile phones. Recognising the inherent privacy risks associated with access to various phone resources (Wi-Fi, GPS, microphone), PRISM applies resource metering to monitor resource usage and determine associated data usage. To combat malicious applications releasing sensitive data, 'forced amnesia' is applied where the phone's application state is reset and data wiped periodically to reduce the ability to accumulate sensitive data, assuming most participatory sensing applications will upload aggregated or converted data (such as noise level rather than audio stream). To ensure scalability of the system, PRISM trades off a degree of privacy and enables the system to push data onto the network rather than the pull system of the more privacy aware Anonysense platform (Cornelius and al. 2008). These steps highlight the need for additional privacy and security measures when providing access to privacy sensitive sensors and data streams.

Ear-Phone is the implementation of an end-to-end system for participatory sensing, (Rana, Chou, et al., Ear-Phone: An End-to-End Participatory Urban Noise Mapping System 2010). A significant contribution is the evaluation of proposed methods for addressing the problem of missing data samples based on compressive sensing. A fundamental characteristic of people-centric sensing is that continuity of data is not available, so data is always incomplete. Localisation accuracy is addressed by converting GPS data to nominated grid points. A limited deployment was conducted to validate measurement accuracy, where it was demonstrated that the platform could achieve good area coverage for noise profiling with a small number of participants. Additionally, the system proposes context detection capabilities using a variety of in-built sensors, including: call detection; speech detection; and context discovery (phone carrying mode), in order to determine activation and what data should be collected/discarded. This highlights a challenge in preserving user privacy. In this system, the phone's sensors collect raw data (e.g. audio recording) before manipulating or discarding the data. Such approaches assume or require the node (phone) to be operating securely, such that data collected and stored on the phone is adequately protected from attack or access by parallel programs.

3.2 Deployed systems

Whilst most reported PS applications are deployed within a research and development framework, increasingly, PS deployments are extending their reach by also providing limited community services. In Australia, Boroondara Council (suburban Melbourne) has partnered with Deakin University to launch an app for residents to measure traffic noise on the nearby freeway as part of a study targeting noise occurring between 10pm and 7am. The study utilises PS to specifically analyse noise levels detected within dwellings. Results are uploaded to a server and then shared through mapping (2Loud 2013)

The EU FP7 project SmartSantander (SmartSantander 2013), saw the establishment of an Internet of Things testbed, consisting of thousands of sensor nodes deployed around the Spanish city of Santander (with linked deployments across Europe). This testbed simultaneously functions as research infrastructure and a service provision platform, serving the needs of both researchers and city officials. The community are also beneficiaries, through the implementation of PS capabilities and the information generated. Running on Android and iOS platforms, the Pace of the City app has been downloaded thousands of times. Its primary functions are the collection and transmission of the phone's sensor samples to the SmartSantander platform, as well as allowing citizens to report on events, and shared with other users. For example, traffic hazards or damaged infrastructure can be reported (and accompanied by evidence, such as pictures). This functionality has seen a large increase in the number of reported events, demonstrating the effectiveness of PS as a reporting tool and subsequently citizen engagement, as Council is then compelled to respond to these notifications by addressing the problem, with measureable time to resolution.

The different schemes variously apply some type of security and privacy measures. These consider typical user perceptions regarding personal privacy. However, they generally make certain assumptions about the user preferences and effectively apply a one size fits all approach.

In (Broenink and al. 2010), a proof of concept system is reported that utilises Near Field Communications (NFC) capabilities of selected smart phones to detect nearby RFID tagged devices. It refers to the user's preset privacy preferences and subsequently informs the user of the correlation between their own and the privacy policy associated with the given product, so enabling informed decision-making.

The relationship between privacy and security capabilities, user preferences and impacts on user engagement and ongoing participation are more complex and require further attention.

3.3 Key points

- **Noise management is essential to prevent health impacts and preserve quality of life**
- **Smartphones can provide indicative measures of noise, but require calibration strategies for the data to be usable**
- **Data collection (sound, location) and handling (mobile device and associated cloud services) must reflect privacy principles**
- **Data quality remains greatly affected by user performance**
- **Early deployments have respectively demonstrated selected capabilities, yet a comprehensive and flexible system catering to diverse needs and perceptions is still required**

4 Privacy vs Transparency

A commonly understood definition of privacy is the right to have one's personal environment (and information contained therein) protected from intrusion. In this way, it is also interpreted as the right to be left alone (Brandeis and Warren 1890). Indeed a focus of this view by Brandeis and Warren in 1890, was in the provision of compensation of suffering resulting from privacy invasion, and so drew attention to dignitary harms (such as reputation) (Kesan, Hayes and Bashir 2013). Alternatively, in the modern context, it can be defined as control over personal information (Shilton and Estrin, Ethical Issues in Participatory Sensing 2012). It implicitly draws a contrast between what constitutes private space and public space and the subsequent delineation of private information versus public information. It also draws into question the status of private activity that necessarily crosses over to public spaces. To appreciate the significance of privacy protection, the function of privacy in a societal context "protects situated practices of boundary management through which the capacity for self-determination develops," while "conditions of diminished privacy also impair the capacity to innovate" (Cohen 2013).

With specific reference to participatory sensing, privacy has been interpreted as "the guarantee that participants maintain control over the release of their sensitive information" including "protection of information that can be inferred from both the sensor readings themselves as well as from the interaction of the users with the participatory sensing system." (Christin, Reinhardt, et al. 2011).

Formal definitions have been established with reference to what is protected by law. As such, it varies in differing degrees according to the jurisdiction to which the law is being applied. According to the Victorian Government Privacy Commissioner, the common element is the ability to keep "your own actions, conversations, information and movements free from public knowledge and attention." This can be interpreted differently in the context of the home, workspace or other environments. Importantly, associated legislation only covers certain types of information and activities. It is important to recognise that protections tied explicitly to identity are inadequate, as enough consolidated information may be used to identify an individual's activities, locations and relationships and in that way leaves them vulnerable to exploitation, without ever requiring the establishment of identity (Wright, et al. 2009).

To appreciate the legal boundaries applied in privacy law, it is necessary to acknowledge that it is different from both confidentiality and secrecy. Confidentiality in legal terms relates to information given under the obligation that it not be shared further. Such information is not usually publically available or easily accessed. Secrecy relates to the prevention of information becoming known, where such action may assist in privacy protection or in serving the public interest.

Limitations of existing US legal frameworks to effect genuine protections through combinations of privacy, data protection and communications laws, have been explored in (Bast and Brown 2013). In light of the inability to singularly protect privacy in that context, a combined approach is recommended that employs education, empowerment and enforcement (where available) (Thierer 2013).

4.1 Ethics in Design

Ideally, privacy safeguards embedded in the system design should give users the necessary control over the collection and release of their data. However, the personal nature of PS as well as the proximity to other persons not actively participating in the PS program raises certain complications. In this respect, it is important to consider alongside privacy, the notions of consent, equity and social forgetting (Shilton and Estrin, Ethical Issues in Participatory Sensing 2012).

Balancing the need for privacy and proposed means for satisfying it raises further questions about the fundamental ethics being applied and about the strength of those ethical principles when considered in the light of seemingly necessary compromise. When such principles are applied at the design level, applied haphazardly, or not applied at all, the implications for the user are likely to be an increased vulnerability from having shared revealing data and for the organisers, exposure from basing released information on inaccurate and possibly malicious data.

Design objectives can be easily placed in opposition as a means of more easily arriving at a certain outcome. For example, **privacy versus accuracy** has been proposed as such a compromise, where in order to preserve some degree of privacy, it has been suggested to perturb data supplied to the system in order to mask the real data that reveals perhaps the actual location or actual time at which samples were collected. Consideration must be given to how this is achieved. If the granularity of the data is merely reduced, it is more a reflection of the preparedness of the user to supply a certain level of detail. Therefore, it is not the accuracy of the data in question, but rather the quality. Transparency in the system ensures that the error margin or data granularity is known, such that subsequent operations on this data can factor in the associated data quality. This is different from intentionally supplying incorrect data, albeit with the same intention to mask activity or identity. In this instance, there is little recourse to separate legitimate users from malicious users, as both courses of action seek to bias the data pool.

Social forgetting is raised in (Shilton and Estrin, Ethical Issues in Participatory Sensing 2012) as another element of the system necessary to reflect the broader principles at stake. PS presents the possibility for a historical archive of activity. The social media generation are slowly becoming aware of the longer term impacts of seemingly frivolous sharing of photos or posts, as what may be considered private moments suitable for perhaps a circle of friends is not seen in the same light by current or potential employers. As many as 17% of Australians regret something they have posted on a social networking site (increasing to 33% for young people) (OAIC, Community attitudes to privacy survey 2013). It has been suggested that such long-term recording and retention, reduces the capacity for a fresh start, or to be able to recover from one's mistakes. In the US, this has been referred to as the "Eraser button" approach, whilst a similar EU version refers to a "Right to be forgotten" (Thierer 2013). As raised in the analysis of reputation management, to what extent does recent activity predict future behaviour compared with more distant activity? In that context the challenge was, rather, how to establish reputation quickly in the absence of historical data. Also important, is the duration of data and activity retention, and associated weighting applied in determining other factors such as reputation. In this instance, it becomes a factor for the user in establishing a trust that they (and their data) will be treated fairly and justly (Shilton and Estrin, Ethical Issues in Participatory Sensing 2012). Mechanisms exist within law to address such issues, so measures must surely be applied to extend such a capacity to emerging technologies that in principle seek to reflect social systems.

System transparency also applies where **user consent** is concerned. It is essential that where users are relied upon to actively participate in the sensing process, adequate consent be obtained for the utilisation of associated data contributions. This is challenging in an environment that by its nature encroaches upon people's personal environments and furthermore by the degree of consent which may be obtained. Active and informed consent is essential if any sort of parity between users and organisers is to be established. As noted earlier in the challenge of overly complex Terms of Service Agreements, it is difficult to infer the level of understanding reached by a user in order to obtained informed consent. However, the level of consent can be qualified and ranges from:

- Passive consent – where utilisation of the platform implies consent given, and so utilised by organisers to extract content at will (so called 'soft surveillance' (Shilton and Estrin, Ethical Issues in Participatory Sensing 2012)).
- Active consent – requires some action by the user to acknowledge agreement (standard TOS agreement), but does not necessarily indicate understanding, rather places responsibility upon the user.
- Qualified consent - contingent on circumstances specified by users or guarantees provided by organisers, with the system operation reflecting selected preferences.
- Informed consent – effective communication of usage conditions and implications, with consent elicited in a manner that reflects the level of understanding and agreement.

The extent of the implications and subsequent agreement required still needs to be explored in order to establish the level of risk that applies to each of the stakeholders. This can be extended to include a more thorough analysis of demographics within stakeholder groups, particularly where it concerns more vulnerable participants. Where the implications impact only the individual user, the direct and active consent suffices. However, where sensing applications increasingly extend to environments shared with others (be they private or public, home or work) the same mechanism may no longer be adequate. The system may protect the privacy of the user, but what of bystanders who may have no knowledge of sensing taking place, no knowledge of implications and potentially different views on the conditions for qualified consent. Is the user in a position to take responsibility for the privacy of people within the vicinity of the sensing system? The significance of these flow-on effects is dependent on the type of sensing taking place. In any case, due consideration must be given to these impacts in the design and in communicating any vulnerabilities to the user.

In order to establish trust, organisers need to be able to provide assurances of how the data is used, whilst system designers embed related functionality within the design. Where insufficient trust exists between users and organisers, users can still have the option of reducing the granularity of data shared or applying some other means of anonymisation (such that the supplied data may still contribute something meaningful).

In the context of citizen engagement and promoting interactive government, applying such procedures is a means for demonstrating transparency and for growing trust. The functionality of the PS platform then enables users to better understand the significance of risk factors as well as the measures applied by organisers (e.g. government) to mitigate such risks. It is ultimately the responsibility of the system operator to adequately inform users, particularly in the absence of adequate risk mitigation and vulnerabilities being exposed.

In determining the viability of such deployments, it must be established whether the introduction of such technology platforms is potentially increasing the vulnerability of particular demographics, or whether through careful design and deployment it acts to reduce such vulnerabilities. Whilst as many as 60% of Australian youth acknowledge the privacy risk of personal information and online services (OAIC, Community attitudes to privacy survey 2013), this still leaves too large a number unaware of the implications associated with what they perceive as ordinary online activity. If it is not possible at the development stage to mitigate these risks, than it may still serve this purpose by providing effective and explicit information transfer relating to the data sharing risks.

4.2 User perceptions

Requiring further investigation is the existing knowledge level of such issues as well as the relationship of risk awareness to participation rates.

Research by the Australian Communications and Media Authority (ACMA) has found increasing concern regarding security and privacy amongst mobile and online platform users. This is reflected in user online behaviour, where users commonly employ different **digital identities** (transactional, social and personal) as a proactive means for restricting access to personal information. In these different scenarios, users were more or less willing to contribute detailed identity information, responding to information demands by going elsewhere for the same service, or even providing misleading information (defensive inaccuracy). In this way, some users could be found exercising their own balance of data integrity and pseudonymity (ACMA, Digital footprints and identities Community attitudinal research 2013). At the same time, whilst nearly 40% of respondents were confident they could effect their desired privacy level through available privacy setting options, another 40% were only hopeful that this was the case, with remaining number holding a negative view.

More than two-thirds were concerned about the level of information shared when using location-based services. Other important findings, included: increased usage does not translate to greater understanding; risks are poorly understood; knowledge of risks and available protections were poor; and users desired more information to assist them to protect personal data (ACMA, Here, there and everywhere—Consumer behaviour and location services 2012).

There was found to be substantial **trust** in government and established banks for securing transactions and using them only for legitimate purposes. Significant trust and responsibility for managing and policing digital identity and breaches was still placed in government. The distinct roles of individual stakeholders have also been acknowledged, with: individuals having primary responsibility for protecting their personal information; service providers and industry operators responsible for enabling a secure environment; and government providing information and education services, raising awareness and enforcing safeguards (ACMA, Here, there and everywhere—Consumer behaviour and location services 2012). Indeed, high standards of transparency in data handling are also universally expected from all organisations, as well as demands for notification of handling breaches and protection and management practices (OAIC, Community attitudes to privacy survey 2013).

Similar studies of mobile user attitudes to privacy conducted by other agencies across Australia and around the world have also revealed concerns for users of mobile and online platforms. This includes apps that do not intrinsically incorporate data sharing.

GSMA studies of mobile user attitudes to privacy conducted across the UK, Spain and Singapore, with follow-up studies in Malaysia, Indonesia, Mexico, Columbia and Brazil, found that approximately half of the respondents expressed concern about sharing personal data whilst using mobile online services or apps, with over three quarters subsequently very selective about who they shared such information with. Before sharing location information of mobile phones, as many as 81% of people wanted their permission to be requested. It was also noted that most users took less security/privacy precautions when using mobile devices compared with PC use. Interestingly, 47% of users would change their usage behaviour if apps were found to use their personal information without consent, whilst 41% would limit their use (FutureSight 2011).

The **Office of the Australian Information Commissioner (OAIC) survey** on community attitudes to privacy, revealed some user awareness of privacy risks associated with online activity (OAIC, Community attitudes to privacy survey 2013). This naturally translates (in some degree) to mobile apps. Some of the key findings are noted here.

With respect to personal information, online services are viewed as the biggest privacy risks (including ID fraud and theft, followed by data security). Concerns about handling of personal information are evident in dissatisfaction with such data being sent offshore (with 90% expressing concern). This certainly raises questions about data ownership and the ability to guarantee associated protections according to how this data is handled (including communication and storage).

As many as 78% of Australians dislike having their activities monitored covertly on the internet. Some awareness of this activity exists, with around half respondents of the view that most websites and smartphone apps collect user information. Of those aware of such risks, more are actively seeking to protect their information, with 90% at times declining to provide personal information, 80% first checking website security, 72% clearing browser histories and 62% not using smartphone apps because of related concerns and around 30% providing false names or details.

There is seemingly a point at which user demands for privacy are relaxed or traded, with over a quarter of the population prepared to provide personal information in exchange for improved service or reduced prices.

How much then do breaches of trust by system operators or government affect user perceptions and ongoing behaviour? One third of those surveyed experienced problems with the treatment of their personal information. But while there is a better understanding of ombudsmen schemes, many still aren't aware of reporting or complaint procedures. More trust is placed in government organisations than private companies (with only health and financial institutions exceptions). Due to concerns about the handling of personal information, 60% decided not to interact with a private company. No figures were reported regarding continued engagement with given organisations following a data breach.

Efforts to embed privacy with associated guarantees, means of retribution or compensation for data breaches and adequate transparency of data usage all surely contribute to building or rebuilding trust between different stakeholders. In this way, robust technological and policy frameworks for emerging ICT are essential. Participatory sensing is one such capability that occupies a unique space that can mutually benefit users and organisers, if implemented accordingly. Implemented haphazardly, it simply reflects the existing flaws and lopsided exchange dynamics that often exist respectively between users, commercial operators and governments. It goes one step further than straight forward app development principles. Likewise, it extends beyond activities of disengaged mass-surveillance, principally because it actively engages the user to contribute data and collection resources. So, the respective parties enter into an agreement or contract for the exchange of information. The user is only able to provide informed consent if they are made adequately aware of the system's operation and their associated role and rights in interacting with the system.

4.3 Key points

- **Privacy is one's control over access and flow of their information**
- **Legal protections are limited to specific circumstances**
- **Ethical means for privacy protection offer transparency with respect to data accuracy and embed privacy in the design**
- **System transparency and verifiable privacy measures can build trust**
- **Social implications warrant mechanisms for managing data history**
- **Informed user consent needs to be the goal and supported by effective communication of risks**
- **Users will utilise various means for protecting privacy, according to their level of awareness and evaluation of risks**

5 Policy frameworks

The protection of personal information by government organisations is paramount in maintaining the trust of its citizens. It is necessary then for such organisations to have in place effective policy frameworks that detail procedures for collection, handling, retention and deletion of personal (and sensitive) information. As well, citizens need to have available recourse to some authority when breaches of this trust take place. In the case of local councils, the UK Information Commissioner's Office (ICO) reported that this particular sector received over £2m in penalties over the last three years following discoveries of serious flaws and errors in personal data handling procedures (Monaghan 2013). Common errors included personal or sensitive information being sent to the wrong person, unencrypted portable data storage and inadvertent online publishing.

Whilst internal government policy may provide the necessary assurances and quality of service for activities in which local government is directly involved or responsible for provision of given services, the same level of control does not exist for external commercial services or PS applications. Such instances rely instead on legislation enforced by the associated controlling or licensing authority; or on industry self-regulation. Where these services are contracted or out-sourced by local government, then contractual guarantees may be included in service level agreements. In such cases, the user is reliant on the local government or equivalent organisation to enforce adherence to such agreements, and so the trust relationship is established between the user and the organiser (local government), rather than the platform developer.

5.1 Privacy standards

As mentioned earlier, varying definitions for privacy exist according to the particular jurisdiction. In the UK the Data Protection Act 1998 (DPA) is concerned with 'personal data' meaning: data which relate to a living individual who can be identified—

a) from those data, or

b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

The UK's ICO also provides a **code of practice for anonymisation** of personal data in support of the DPA (ICO, Anonymisation: managing data protection risk code of practice 2012). Recognising that with the increasing accessibility of data in the public domain, the ability to piece together disparate sources of information to paint a more detailed picture of the modern world also offers the prospect for combining multiple data sources to reveal previously hidden (or at least separated) aspects of personal information. The code of practice seeks to overcome the weaker protections that apply to already anonymised data. Anonymised data refers to data that does not of itself reveal identity and is unlikely to do so through combination with other data (re-identification). It is noted that it is not possible to establish absolute re-identification risk, but recommends procedures to ensure that the prospect is at least remote. Implementation of the code is also presented as an example of privacy by design.

The ***Australian Privacy Act*** regulates how entities handle individuals' personal information as well as apply necessary steps to protect such information. It defines Personal Information as:

> Information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or an opinion.

Within the *Privacy Act*, Sensitive Information about an individual, which demands specific attention, includes:

a) information or an opinion about an individual: including racial or ethnic origin; political opinions; membership of a political association; (among other things), that are also personal information;

b) health information;

c) other genetic information.

Additionally, the OAIC provides a set of **Australian Privacy Principles** superseding existing Information Privacy Principles and National Privacy Principles from March 2014. Details are contained within the Privacy Amendment (Enhancing Privacy Protection) Act 2012, which amends the 1988 *Privacy Act* and applies to organisations and federal government entities (among others).

Some of the APPs include details and requirements for the following actions relating to the sourcing and handling of personal information:

- Open and transparent handling of personal information (APP 1)
- Anonymity and pseudonymity options (APP 2)
- Collection of solicited personal information (APP 3)
- Notification of collection of personal information (APP 5)
- Use or disclosure of personal information (APP 6)
- Cross border disclosure (APP 8)
- Quality requirements of personal information (APP 10)
- Security of personal information (APP 11)
- Access to personal information (APP 12)
- Correction of personal information (APP 13)

The APA requires organisations to satisfy the APPs by taking reasonable steps to protect and ensure the privacy of individuals and their personal information.

5.2 Operational requirements

Operational requirements of data collection and related activities are varied and apply across a number of different areas. Governmental requirements with respect to data quality, integrity, reliability and validity vary according to the operational needs of given areas and levels of government. Adequate policy frameworks are necessary to detail these requirements in order to meet the needs of government, protect the interests of citizens and ensure the transfer of information between the two is such that the integrity of the communication and information is preserved.

5.2.1 *Data collection and management*

With respect to the collection and handling of personal information, the City of Melbourne, as detailed in its Information Privacy Policy Statement, adheres to the requirements of the Victorian Government *Information Privacy Act* 2000 that covers State government organisations, local councils and private organisations contracted by government. Viewing the protection of an individual's privacy as integral to its commitment towards accountability and integrity, the City council's policy covers its Councillors, officers and contractors.

Personal information is closely managed in accordance with 10 Information Privacy Principles. Of significance is the commitment to:

- Only collect personal information (ideally only from the person to whom it relates) when it is necessary to do so to facilitate a specific service (e.g. contact you where necessary; supply material; facilitate collection of fees; enable payment for Council services; undertake law enforcement; aid community safety) (re. IPP 1)
- Protect against disclosure of personal information (without prior consent, unless authorised by law) (re. IPP 2)
- Maintain accuracy and security of information – Data Quality and Security (re. IPP 3 & 4)
- Openness and transparency of procedures (re. IPP 5)
- Allow for anonymity in communication (re. IPP 8)
- Specific conditions for trans-border data flows and sensitive information (re. IPP 9 & 10)

Responsibilities also include: always informing individuals how their information will be used and disclosed; only using it for the primary purpose for which it was collected or a secondary purpose that would be reasonably expected by the individual. This protects against over-collection. Additional measures for security of collected data, apply not just to storage, but also to adequate security of devices (computers, portable storage devices, workspaces) utilised in working with personal information. Similar guidelines are provided for the secure storage, disposal or de-identification of primary identification and other sensitive documents.

Of particular relevance to any application of PS is the sensing medium that itself may reveal personal information. As such, also considered personal information are photographs, video and voice recordings from which a person's identity can be reasonably established. Where it is impractical to obtain individual informed or written consent (such as large events or gatherings), adequately displayed notification is recommended. Such measures allow individuals to reconsider their participation, or where requests for images not to be used for publication are expressed, exploration of editing measures or omission of the data in question.

In the noise mapping context, varying data quality needs can be seen for example across:

a) city planners – where soundscape knowledge may be enhanced by contextual information sourced through citizen feedback;

b) compliance officers – where accurate measurement data as well as specific times, locations and the nature of events may assist responses to noise complaints

c) Councils – for whom comprehensive noise maps may inform appropriate zoning, public space utilisation and related policy and strategic planning decisions.

In terms of specific requirements associated with PS as a noise management tool, certain technical challenges remain for it to be broadly applied across different levels of council operations. These include:

5.2.1.1 *Soundscape mapping*

- The challenge of attracting sufficient participants applies here. This goal utilises the subjective feedback capability of PS together with the objective sensor measurements in a way that provides reference points to classify user interpretations of perceived noise levels. The challenge is in drawing sufficiently diverse participants to remove demographic bias in categorizing the local soundscape. In this instance, the recruitment strategies described earlier may address this problem.

5.2.1.2 *Noise complaints system*

- Noise PS offers the potential to collect real-time data (and thus evidence) associated with noise complaints. Such data may include SPL (noise level), time, location, description and impact. These can be supplied with the complaint to validate user perceptions and offer council officers more detail to enable complaint resolution. The challenge here is the quality of the associated data. In particular, location based on GPS readings or Wi-Fi hotspot locations are problematic, particularly in built up areas such as the city CBD, as the error margin for such readings are too large to produce verifiable localisation for noise sources. Advanced localisation strategies are required if the PS location data is to be used as an objective sensor reading. Limitations of sensing hardware (calibration accuracy) remains a challenge, though recent strategies reported in the literature go some way to addressing this. Secondly, the user influence in collecting good quality sensor data may also limit the objective evidence potential of the collected data, as it is difficult to verify the circumstances under which the samples are collected. Without resolving such issues, the role of PS in this scenario merely supplements the complaint details, without necessarily supplying independent verifiable noise data. Only fixed infrastructure noise monitoring can provide this functionality (against which PS data can be calibrated/validated). The traditional council methods for verifying the noise event are still required.

5.2.1.3 *Noise mapping*

- Compared with the standard noise modelling methods applied around the world to satisfy government noise mapping directives, and additional measured noise data must surely be advantageous. For the inclusion of PS based data into the model, data validation strategies must be applied. This must consider user proficiency in collecting data samples, compensating for weather factors, proximity to noise source, positioning of microphone and other variables affecting sample quality. This may be mitigated somewhat through data aggregation from multiple participants together with reputation management strategies to weight data accordingly. Additionally, other sensors may provide sufficient data with respect to the measurement conditions, to ensure that data bias is reduced as much as possible.

5.2.2 *Citizen Engagement*

In addition to providing service guarantees and privacy protections to establish trust and attract participation, government also has the responsibility of providing equitable access to engagement programs. In this regard, inadequate privacy provisions that act to deter citizen engagement can be interpreted as a form of exclusion for a segment of the community (Wright, et al. 2009). This can easily extend to exclusion from available services and is thus further motivation to remove potential barriers to participation.

In the context of potential PS deployment applications, the City of Melbourne (CoM) already employs various strategies for engagement, termed 'community engagement' (CE) and sourcing feedback on issues, that may similarly serve dedicated PS campaigns, or indeed, PS may yet serve as a supplement to existing engagement practices. Community engagement in this context is "any process that involves the (impacted and interested) public in problem solving or decision making and uses public input to make decisions." This is precisely the objective of PS whilst also delivering the medium through which this engagement takes place. The City of Melbourne CE Framework links closely with the values and ethics of the International Association for Public Participation (IAP2). Some of these values include:

- the belief that those affected by a decision have a right to involvement in the decision-making process;
- the promise that the public's contribution will offer influence;
- recognition of needs of all stakeholders;
- seeking involvement of those affected;
- facilitating meaningful participation; and informing of the impact of participant contributions.

The IAP2 details a spectrum of public participation, with objectives that correspond to the increasing level of public impact. This spans objectives to: inform, consult, involve, collaborate and/or empower the public, with each having a corresponding participation goal, promise to the public and example tools for engagement.

The City receives feedback on issues and topics of interest through a variety of means, including: on-line surveys (via the Participate Melbourne platform (CoM, Participate Melbourne 2014)), hand out questionnaires, focus groups, face to face forums, open house meetings, pop ups, vox-pops, deliberative forums and random selection processes. Many engagement processes (Participate

Melbourne registration or community meetings) do require some personal information to be supplied. Additional detail may be requested to assist organisers in refining where necessary the sample group, to obtain broader representation for example.

The particular process undertaken varies according the complexity of the issue/opportunity, the risk associated with the issue and the level of resources available to undertake the process. The process duration is similarly variable, for example: a one-off 2-hour focus group or a 2-week on-line community forum. A deliberative process extends further, perhaps involving the same group of people in ongoing conversation for several months and will frequently involve multiple simultaneous processes. The impact of the given CE process often corresponds to the level of community influence in the issue/opportunity, on both the participant and the sponsoring body.

Feedback is reviewed and where relevant to the issue, policy or program in question, it is explored in more detail with further information sourced where needed. This material is then directed into the final engagement report. In completing the CE process, the feedback is fed into the decision making processes of council. Those involved are also informed of the outcomes of the decision making process and undertake an evaluation of the CE process.

Importantly, the feedback comes from a variety of community members and is based upon their opinions or experiences. This offers the rationale for quality processes that draw upon empirical data so that participants can develop ‘informed opinions’. Diversity is essential – as informed opinions from a variety of community members help to build a larger ‘window of knowledge’ from which decision makers can draw. It is at this stage that themes and patterns are seen to emerge. The PS framework reflects all of these principles and may therefore complement such endeavours by also collecting objective data to further expand the knowledge base, at the same time as providing a medium to serve some existing CE requirements.

5.2.3 *Complaints handling*

Processing citizen feedback is also a responsibility of Customer Relations and processed according to the nature of the feedback. When the feedback is in the form of a complaint, CoM applies complaint-handling procedures framed by the Victorian Ombudsman (Brouwer 2007). Key factors in assessing the effectiveness of implemented policy are:

- Committed management
- Authorised and trained staff
- Empowered and informed clients
- Recording and analysis of complaints data

When applied well, these procedures should result in: improved business practice; better corporate governance; and better client relations.

Depending on the nature of the complaint, certain information is required to ensure effective processing and greater likelihood of resolution. The corresponding privacy policy once again applies, so personal information supplied with the complaint may not be necessary in all instances, however, it will allow follow-up by council officers and requests for more detail if required. In the context of noise mapping, once a complaint is registered, officers must determine the appropriate legislation under which the incident falls in order to refer the action to the appropriate authority. This is a unique feature of noise management in the Australian landscape in that depending on the nature of the noise, different legislation and government authorities are responsible for managing it. For example, aircraft noise is a federal government responsibility; traffic noise crosses both federal and state legislation, whilst management falls to the state roads authority; residential noise is a state government responsibility; whilst local council is responsible for managing noise issues that correspond to permits and hours of operation. The latter commonly encompasses: licensed venues; public address systems; construction or industrial operation related noise; waste collection; among others. This is a simplified insight into the convoluted nature of noise management that is enacted by state police, the state Environmental Protection Authority (EPA) and local council officers.

It should be recognised that whilst effective complaint handling practices deliver satisfactory customer service, it is a constrained medium through which to measure customer satisfaction, as it is predominantly dissatisfied customers who employ this communication channel.

With respect to breaches of personal information security, the individual has recourse to complain to the federal government's Office of the Australian Information Commissioner (OAIC), if the matter could not be resolved through direct contact with the agency or organisation in question (who is covered by the Privacy Act). The OAIC may investigate and may attempt to resolve the matter by conciliation between the parties (OAIC, Data breach notification: a guide to handling personal information security breaches 2012). The Privacy Act does not impose specific penalties for breaches, yet the Commissioner may make determinations requiring the financial compensation for damages (or other remedies, e.g. issue of an apology), which in turn can be enforced by the Federal Court or Federal Magistrates Court.

With the aim of promoting transparency and building trust, the GSMA has proposed an accountability framework for organisations. They promote accountability as "the commitment to, and acceptance of, responsibility for protecting personal information in compliance with laws or other standards" together with the ability to demonstrate compliance (GSMA, Accountability Framework for the implementation of the GSMA Privacy Design Guidelines for Mobile App Development 2013). Key elements include: organisational commitment; internal program controls (mechanisms) for giving effect to the guidelines; and enforcement for noncompliant organisations.

5.3 Industry self-regulation

Faced with the complexity of providing adequate privacy protection through legislative frameworks, a number of privacy authorities and industry associations are advocating a suite of solutions that might best enable a balance of stakeholder interests. **Privacy by design** is one piece of this puzzle, that is being recommended by UK's ICO (ICO, Privacy by Design 2008), as well as Australia's OAIC. It promotes due consideration of privacy risks throughout the design process, through engagement with stakeholders. Key recommendations include the establishment or development of:

- An executive mandate
- Privacy impact assessments (PIA) throughout the system lifecycle
- Cross-sector data sharing standards
- Practical privacy standards
- Promoting privacy enhancing technologies (PET) research
- Rigorous compliance and enforcement mechanisms

Such actions, it is hoped, will redress the negative perception of organisations as collecting too much information and retaining data for longer than necessary. Privacy Impact Assessments (PIA) facilitate this by changing the mentality of organisations to move beyond legislative compliance checklists and instead consider broader privacy implications, in view of community perceptions and expectations, before systems are deployed. In a study of PIA implementations and effectiveness across the UK, Australia, Canada, New Zealand, Hong Kong and the United States, variability was observed in perspectives and implementations of PIAs across different levels of government, and jurisdictions (Bennett and Bayley 2007). It was shown to be a valuable process, itself transparent and accountable. The OAIC specifies five key PIA stages as:

- Project description
- Mapping information flows and the privacy framework
- Privacy impact analysis
- Privacy management
- Recommendations

Each element is adapted to the particular needs of the project in question (OAIC, Privacy Impact Assessment Guide 2010).

To address the specific privacy challenges raised through increasing use and functionality of smart phones, the GSMA, ICO and OAIC have respectively produced **design guidelines for mobile app developers** to focus their attention on these critical issues (GSMA, Privacy Design Guidelines for Mobile Application Development 2012) (ICO, Privacy in Mobile Apps: Guidance for app developers 2013) (OAIC, Mobile Privacy: a better practice guide for mobile app developers 2013). They adopt a privacy by design approach and attempt to foster a development environment, encompassing the entire service delivery chain (developers, manufacturers, OS platforms, mobile operators, advertisers and analytics companies) to engender trust and confidence, based on the provision of transparency, choice and control (GSMA, Privacy Design Guidelines for Mobile Application Development 2012). In one respect, it alters the commercial imperative by putting the customer first. Importantly, the OAIC guideline draws attention to the developer’s obligations under the Privacy Act. It also draws attention to the challenge of communicating necessary information to the user via the phone interface.

While direct regulation and strong policy frameworks will continue to play a role, the global nature of the supply chain means there will remain a substantial reliance on self-regulation and direct communication to consumers to equip them with the knowledge and control to exercise necessary protections (ACMA, Mobile apps—Emerging issues in media and communications 2013).

5.4 Key points

- **Systems for protection of personal information are essential for maintain/building trust between organisations and citizens**
- **This includes discovery of breaches and recourse for compensation**
- **Existing policies cover data collection and handling; citizen engagement strategies; and feedback management**
- **They reflect privacy concerns; principles of open and responsive government; and value in citizen contributions to governance**
- **Limitations of privacy legislation demands supplementary principles/guidelines for system implementation, including industry self-regulation, privacy by design and PIA**
- **Elements of each need to be utilised and adapted for PS**

6 Pilot Study

Further exploring the many challenges and proposed solutions described throughout this paper, a demonstration mobile application (app) has been developed. The app is developed for noise monitoring and provides users with a tool for measuring the sound pressure level (SPL), together with the ability to annotate the measurements with contextual information. Data is then able to be uploaded to a central server, where the data can be analysed, consolidated, mapped and visualised for consumption by a given audience. In the proposed architecture, we propose to include a spare mobile participatory sensing layer for noise data collection (Gubbi, Marusic, et al. 2013). To this effect, the app was developed for the Android platform. The app was created using Eclipse and Android Developer tool (Android 4.2.2) for HTC Desire X mobile phone. The data in Table 2 was collected from each user according to privacy levels defined in Table 3. The data collected is stored in the phone and uploaded to the Cloud server for analysis.

Data	Description
Noise levels	Noise level
Location	GPS/AGPS (radius X metres)
Time	Store time
Battery	Measure usage
MAC / physical address	Store physical address
Phone Number and ID	Store number and ID
Movement (accelerometer)	All
Nearby wireless devices	Detect & store no., type and ID
Requested User Input:	
• **No. people in vicinity**	Input number
• **Effect on mood**	(Positive) … (Negative)
• **Event/environment**	User input

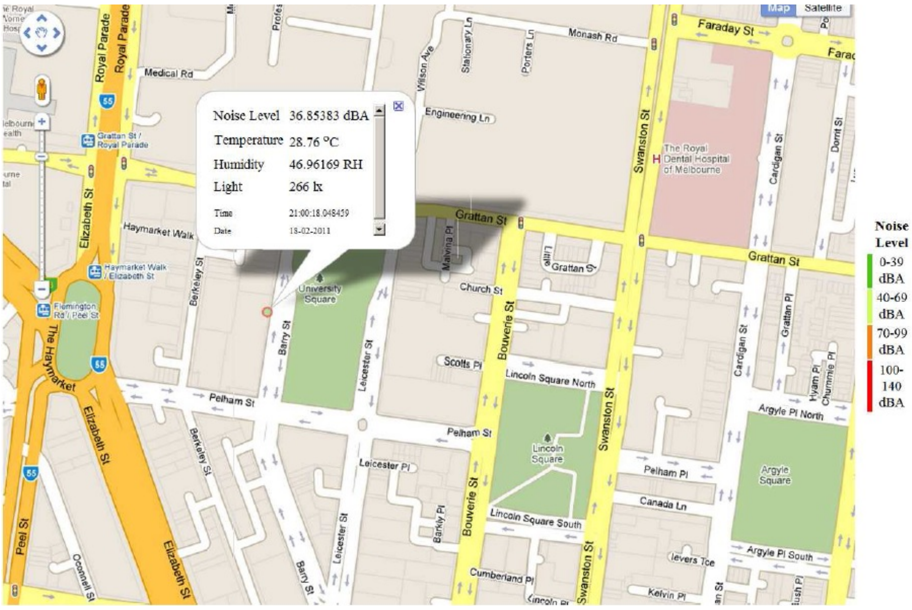
Table 2: Data collected for participatory sensing

Privacy Level 1 (No privacy)	Privacy Level 2 (Some privacy)	Privacy Level 3 (Neutral)	Privacy Level 4 (High privacy)	Privacy Level 5 (Private)
• Maximum noise level will be collected every second for 1 minute • Your GPS location will be stored • Your MAC ID, Time, Phone number and Bluetooth devices in the vicinity will be recorded • Your movements will be monitored for 1 minute.	• Maximum noise level will be collected every 2 secs for 1 minute • Your GPS location will be stored • Your MAC ID, Time, Phone number and Bluetooth devices in the vicinity will be recorded • Your movements (maximum, average) will be recorded every 2 seconds for 1 minute.	• Maximum noise level will be collected every 5 secs for 1 minute • Your approximate GPS location will be stored (2 km radius) • Your Time and Bluetooth devices in the vicinity will be recorded • Your movements (maximum, average) will be recorded every 10 seconds for 1 minute.	• Maximum noise level will be collected every 30 secs for 1 minute • Your approximate GPS location at city level will be stored • Your Time and Bluetooth devices in the vicinity will be recorded • Your movements (maximum, average) will be recorded every 30 seconds for 1 minute.	• This level blocks all information from being stored

Table 3: Privacy levels used and description provided to the user

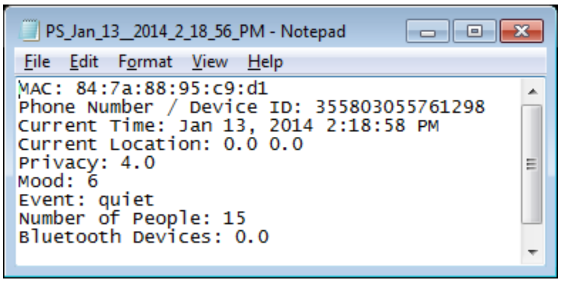
6.1 Visualization

Once the data is collected, the data is stored in the cloud. Currently, the noise data is being stored in the Xively server (previously PACHUBE (Pachube n.d.) for analysis at network level. For visualization, the publicly available COSM application is used for the mobile platform. For desktop operation, Google maps are used as shown in Figure 1.



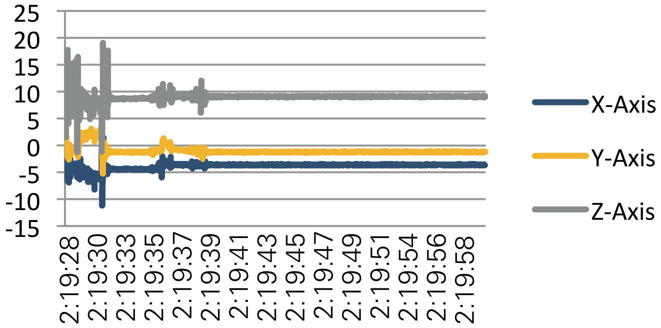
Noise Level 36.85383 dBA
Temperature 28.76 °C
Humidity 46.96169 RH
Light 266 lx
Time 21:00:18.048459
Date 18-02-2011

Figure 1: Noise visualization on Google Maps (Gubbi, Marusic, et al. 2013)



PS_Jan_13__2014_2_18_56_PM - Notepad

```
MAC: 84:7a:88:95:c9:d1
Phone Number / Device ID: 355803055761298
Current Time: Jan 13, 2014 2:18:58 PM
Current Location: 0.0 0.0
Privacy: 4.0
Mood: 6
Event: quiet
Number of People: 15
Bluetooth Devices: 0.0
```



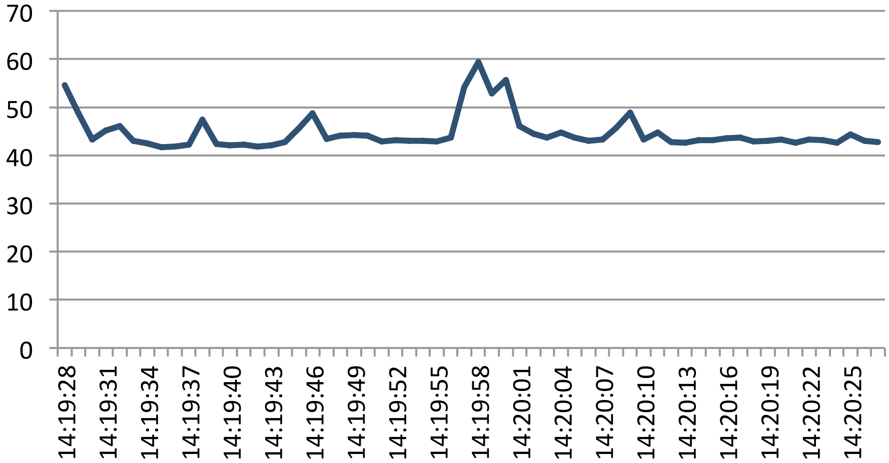
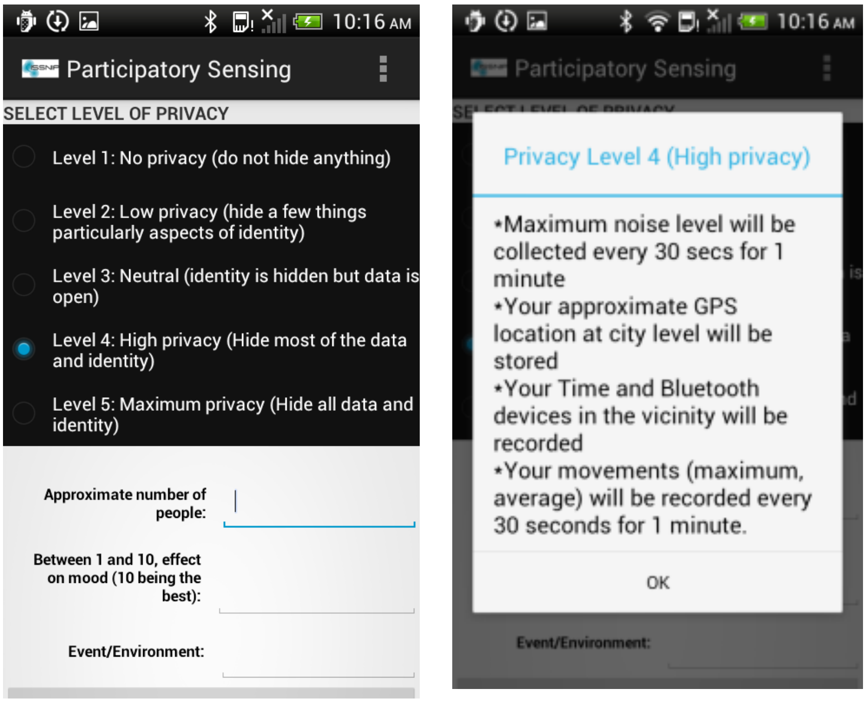


Figure 2. Examples of collected data

Rather than propose a comprehensive noise monitoring and mapping solution (which is beyond the scope of this study), key functions are included that enable certain questions to be addressed or highlighted. Ultimately, a larger trial is necessary to seek feedback from key demographics, as well as providing adequate sample size to reveal user perceptions and experiences with the platform.

As there are numerous barriers to user engagement, the PS demo aims to provide the necessary functionality to explore specific factors. In exploring the issue of privacy vulnerability that exists in social media and data sharing apps, the demo incorporates a privacy preference capability. This enables the user to express their privacy preference, which in turn defines the operation of the sensing platform in terms of the type and volume of data that is collected and shared. In this way, the app serves to inform users of privacy implications (to a certain extent) whilst also specifying the corresponding mode of operation. This represents a degree of transparency that allows the user to be fully informed about the nature of the app and collection of sensor data. The important aspect of this functionality is not merely to demonstrate the technological capability, but rather to provide a tool that measures user preferences, responses to information provision, level of awareness and associated usage behaviour. It seeks to evaluate PS as a communication medium and determine whether such an interface is able to appease privacy concerns and thus improve participation rates.

Given the participation flexibility offered by the proposed platform, as determined by privacy preferences, users can engage with the system in varying degrees. Some users may only wish to collect data for their own personal use. Others may wish to release only limited information (restricting potentially sensitive information). This has implications on the volume of data being collected, resulting in potential gaps at certain quality or detail levels. The impact of this challenge needs to be assessed in practice, at the same time as associated recruitment and incentivisation strategies.



SELECT LEVEL OF PRIVACY

○ Level 1: No privacy (do not hide anything)

○ Level 2: Low privacy (hide a few things particularly aspects of identity)

○ Level 3: Neutral (identity is hidden but data is open)

● Level 4: High privacy (Hide most of the data and identity)

○ Level 5: Maximum privacy (Hide all data and identity)

Approximate number of people:

Between 1 and 10, effect on mood (10 being the best):

Event/Environment:

Privacy Level 4 (High privacy)

•Maximum noise level will be collected every 30 secs for 1 minute
•Your approximate GPS location at city level will be stored
•Your Time and Bluetooth devices in the vicinity will be recorded
•Your movements (maximum, average) will be recorded every 30 seconds for 1 minute.

Figure 3. Privacy level selection

It must be noted that this app was created with a research imperative and is thus intended for use by informed participants acknowledging the collection of additional data required to inform the specific research questions. So participants are engaged in a research trial, not merely a PS program. The evolution of this system into an open PS platform would see a number of technical changes, such as sensor level control by the operating system, as determined by the privacy settings. Presently most PS implementations and indeed apps, simply request the use of a given sensor, from which data is collected and stored. This places different security demands on the app and device in ensuring that the collected data is protected from harvesting by other active apps or attackers. The alternative strategy is for the privacy preferences expressed by the user to be implemented at the kernel level, so that sensitive data is not even collected (where possible) or immediately processed and the raw samples deleted. A similar principle is applied to the measurement of SPL without the collection of audio stream data.

Although currently available apps commonly add a disclaimer noting the type of data being collected, user experience indicates that these details are forgotten over time. In this case, it is more useful to be able to restrict the type of data being provided to the app itself. For instance, an App user may be agreeable to providing location information at the City level (say privacy level 3) but may not be interested in providing accurate location to street level (say privacy level 1). The ideal mechanism for privacy implementation would be that the information from the GPS sensor passed on to the app by the operating system is only at the city level. This will ensure no record of the data is collected or retained in the phone as per the user's privacy level. However, the challenge is how to set these levels for various sensors and data. The app developed here intends to collect user information regarding the appropriate privacy levels that will assist us in formulating a standard for specific types of data.

6.2 Pilot study requirements

In evaluating the potential of PS and noise mapping as a suitable tool for enhancing public participation, the following criteria, as demonstrated in (Evans and Reid 2013), may be applied:

- Place – evaluation of the program's innovation with respect to the institution in question
- Novelty – departure from existing practice (and so providing new insight and functionality)
- Significance – addresses an important problem of concern to local citizens
- Utility – the proposed platform eases some government process or operations
- Effectiveness – produces tangible results for citizens
- Longevity – achieves positive results over an extended period of time
- Transferability – the process is applicable to other application domains or government processes

The proposed platform and application certainly has the potential to fulfil all of the above criteria. Further to this, the capacity for the citizens in question to effectively participate and contribute to the process can be evaluated using the **CLEAR** diagnostic tool (Evans and Reid 2013). It assesses the following characteristics of citizens:

- Resources and knowledge to participate (**C**an do ...)
- Sense of attachment (**L**ike to ...)
- Opportunity for participation (**E**nabled to ...)
- Mobilisation through public agencies and civic channels (**A**sked to ...)
- Evidence of their contributions (**R**esponded to ...)

Similarly, all these criteria can be adequately satisfied, as demonstrated by existing programs such as Participate Melbourne.

However, these criteria alone do not adequately ensure that all citizen concerns and needs are met. Until the issues outlined throughout this paper are sufficiently incorporated into the system design and implementation, the success of the process will always be constrained. Therefore, in recommending a larger PS trial, certain developmental conditions need to be satisfied in accordance with the privacy, data protection and mobile app development guidelines outlined earlier.

- A detailed PIA is required
- Consultation of the OAIC app developers guide.
- Specific consideration given to the functionality of the interface for communicating data protection guarantees, implications and privacy preference options.
- Separate evaluation of incentivisation strategies

The scope of a further study will determine:

- Target (or multiple) demographics
- The need for multiple interface mediums (beyond smartphones, perhaps including tablets, laptops, desktops, public display interfaces in locations of interest)
- Stakeholder meetings/workshops

In assessing the potential of PS to engage citizens in local government activity, the following additional performance indicators are suggested:

- User uptake and participation (compared with traditional engagement tools)
- User experience analysis
- Operational change/efficiency improvements (e.g. response times, number of effective resolutions, customer satisfaction)
- Trust management analysis, via the system interface or independent survey through a secondary communication channel (online survey, participant interview).
- Contrast between PS and existing engagement tools, particularly social media (which is already being utilised by local government).

An expanded trial has the potential to produce integrated environmental information at local and metropolitan scales, as well as detailed strategies for dynamic monitoring of critical areas, enabling councils to take immediate action whenever needed.

6.3 Key points

- **The pilot study is based on a noise measurement app and central server for data aggregation and display**
- **The app provides a spectrum of privacy level options, to be selected by the user, that reflect the type and amount of data to be collected/shared**
- **The privacy level selection interface serves to inform the user of data handling (and implies associated risk), while a refined interface can more explicitly convey this**
- **This capability demonstrates a means for increasing user control over their level of participation**
- **A larger study can expand this capability; provide detailed assessment of public participation capacity; conduct a PIA; reach broader demographics; and further evaluate the issues raised throughout this paper**

7 Conclusion

Emerging technologies are providing ever increasing opportunities to understand our local environments through the collection and analysis of vast amounts of data. The proliferation of ICT and its rapid uptake by citizens is offering unprecedented reach into numerous aspects of everyday living. The ability to utilise mobile ICT, in particular smartphones, as sensing devices from which collected data can be easily shared has made concepts of co-production and citizen science, specifically participatory sensing (PS), not only more attractive to relevant organisations, but potentially viable. Despite this great potential, many issues must be adequately addressed before the respective concerns of the participants (citizens) and the PS system organisers are satisfied. We have considered these challenges through the lens of local government and its engagement with its citizens in simultaneously addressing specific operational and service provision requirements, at the same time as building sufficient trust and value provision to warrant the voluntary participation of citizens and their willingness to share their personal resources and data. By highlighting the challenge of noise management, we have sought to establish the genuine potential for such emerging technologies to enable interactive local governance, by recognising the value to relevant authorities in understanding the subjective experience of the urban soundscape by citizens and the intrinsic role played by citizens in providing this insight in an effective manner.

The key challenges have been identified that affect the realisation of a viable and meaningful IoT platform that bridges the gap between the needs of local government to be able deliver effective services on the basis of rich new information streams and the needs of citizens for a local environment that supports their activities. This is uniquely facilitated by the development of PS as an ICT solution that directly engages the citizen in a way that improves their communication channels to government whilst simultaneously improving operational requirements and processes within government to process and act upon this new information.

Citizen engagement and subsequently empowerment comes about through the establishment of a participatory culture. Applying co-production through citizen science to local democracy, we can obtain user input (through data supply and contextual feedback) in decision making by authorities. A suitably designed interaction framework (such as PS) offers motivation and accountability through understanding of contributions and enhanced social perception.

In addressing user incentivisation, to ensure adequate user participation, we considered the need to remove disincentives, such as concerns about privacy intrusion. There is thus a paramount need to ensure privacy and data integrity for the users supplying data and those using data. Appropriate anonymisation of collected data is critical to enable this function. Simultaneously, the PS organiser (or local government) needs to be able to trust or verify the quality of user supplied content. An appropriately designed platform thus facilitates the establishment and building of trust between stakeholders. In serving interactive local governance, the incorporation of principles of transparency and accountability into the system, ensures that this objective can be satisfied. This can be measured through effectiveness of engagement and satisfaction with privacy provisions and guarantees.

A foundation has been laid to address some of the vital social impacts of PS. At the same time, it provides a framework by which this tool can be effectively utilised to meet government operational requirements from service provision through to policy setting and management. The variety of implications from collection and sharing of personally identifiable information, demands a suite of solutions in order to provide robust protections. These include relevant privacy legislation, guidelines for developers and implementation of privacy by design. Where such protections remain insufficient, greater effort needs to be applied in raising user awareness of associated risks. In this way, they are given the opportunity and flexibility to self-determine their level of engagement. Such an approach implicitly recognises the freedom of the individual to interact in their own way.

Appropriately framed, PS can be an enabler for improving the human experience in an environment. It provides mechanism for information transfer between stakeholders. For authorities, it enhances their capacity to manage public space, while for citizens it informs decision making of how/when to utilise public space. In better managing public spaces, local government aids in fostering a sense of community and desire to utilise given spaces. For this to be realised, the means for engagement needs to be broadly accessible – not explicitly reliant on personal resources to access and leverage the benefits. This can be manifested through different interface platforms (e.g. smartphones, PC, tablet; public displays and interfaces. While citizens may benefit purely from the enhanced service provision, this work is focussed on the capacity of engagement and interaction in the governance process. So accessibility must be considered, particularly to avoid any sample bias that may be introduced by limited demographic reach in the engagement.

These insights become a key enabler for the viability of other smart city programs seeking to utilise PS. To adequately test the effectiveness and application of privacy, access and engagement principles identified here, a larger development trial is necessary. In the noise management context this should include application of PIA, privacy by design and privacy policy to measure the effectiveness and adaption to emerging technologies of operational capabilities. Additionally, a broader study will see the establishment of user preferences and their response to increasing awareness and participation flexibility, made available through the platform.

This study has focused on the potential of participatory sensing to promote improved noise management thereby improving quality of life. It has identified a range of technical, ethical, legal and social issues that need to be addressed and proposed further research to help address them. However, the study also has broader application for policy makers wishing to increase and enhance citizen participation in decision making and to take advantage of technological advances to do so. As identified at the beginning of this report, governments seek to engage citizens for a range of reasons. The current context of fiscal constraint provides an additional and compelling motivation for governments to engage directly with citizens in efforts to address issues of community concern. In this context co-production supported by appropriate technology may have application across a much broader range of policy and service areas. Identifying and taking and advantage of those opportunities requires policy frameworks that provide sufficient incentives and safeguards for citizens, providers and governments as we outline in this report. However it also requires attention to structural and professional boundaries within government that act to support siloed thinking and action and limit engagement and exchange.

Bibliography

2Loud. School of Architecture and Built Environment and School of Information & Business Analytics, Deakin University. 2013. http://www.2loud.net.au.

Abdulmonem, A., and J. Hunter. "Enhancing the quality and trust of citizen science data." *Proc. 6th IEEE International Conference on e-science.* 2010. 81-88.

ACMA. *Digital footprints and identities Community attitudinal research.* Australian Communications and Media Authority, Commonwealth of Australia, 2013.

ACMA. *Here, there and everywhere—Consumer behaviour and location services.* Australian Communications and Media Authority, Commonwealth of Australia, 2012.

ACMA. *Mobile apps—Emerging issues in media and communications.* Australian Communications and Media Authority, 2013.

Anderson, D., T. Henderson, and D. Kotz. "Privacy in Location-Aware Computing Environments." *Pervasive Computing* (IEEE) 6, no. 4 (2007): 64-72.

Andrejevic, M. *iSpy: surveillance and power in the interactive era.* Edited by Lawrence KS. University Press of Kansas, 2007.

Barnes, M., J. Newman, and H. Sullivan. *Power, Participation and Political Renewal.* Bristol: Policy Press, 2007.

Bast, C. M., and C. A. Brown. "Where Has All Our Privacy Gone?" *Journal of Legal Studies in Business* (South Eastern Academy of Legal Studies) 18 (2013): 17-43.

Bélanger, F., and R. E. Crossler. "Privacy in the Digital Age: A Review of Information Privacy Research in Information systems." *MIS Quarterly* 35, no. 4 (December 2011): 1017-1041.

Bennett, C., and R. Bayley. *Privacy Impact Assessments: International Study of their Application and Effects.* UK: Loughborough University and ICO, 2007.

Brandeis, L., and S. Warren. "The Right to Privacy." *Harvard Law Review* 4, no. 5 (1890): 193-220.

Broenink, G., and et. al. "The Privacy Coach: Supporting Customer Privacy in the Internet of Things." *Proc. Workshop What Can the Internet of Things Do for the Citizen?* Radnoud Univ., 2010.

Brouwer, G. E. *Good Practice Guide: Victorian Ombudsman's Guide to complaint handling for Victorian Public Sector Agencies.* Victorian Ombudsman, 2007.

Christin, D., A. Reinhardt, S. S. Kanhere, and M. Hollick. "A Survey on Privacy in Mobile Participatory Sensing Applications." *Journal of Systems and Software* 84, no. 11 (November 2011): 1928-1946.

Christin, D., C. Roßkopf, M. Hollick, L. A. Martucci, and S. S. Kanhere. "IncogniSense: An Anonymity-preserving Reputation Framework for Participatory Sensing Applications." *IEEE International Conference on Pervasive Computing and Communications.* Lugano, 2012. 135-143.

Cohen, J. E. "What is Privacy For?" *Harvard Law Review* 126 (2013): 1904-1933.

CoM. *Participate Melbourne.* City of Melbourne. 2014. http://participate.melbourne.vic.gov.au/participate-melbourne.

CoM. *Urban Health Profile.* City of Melbourne, 2012.

Cornelius, C., and et. al. "AnonySense: Privacy-Aware People-Centric Sensing." *MobiSys.* ACM, 2008.

Das, T., P. Mohan, V. N. Padmanabhan, R. Ramjee, and A. Sharma. "PRISM: Platform for Remote Sensing using Smartphones." *Proceedings of the 8th international conference on Mobile systems, applications, and services* . ACM, 2010. 63-76.

De Cristofaro, E., and C. Soriente. "Participatory Privacy: Enabling Privacy in Participatory Sensing." *IEEE Network*, Jan/Feb 2013: 32-26.

EPA. "EPA Noise Surveys." *Informatin Bulletin*, 2007 October.

Evans, M., and R. Reid. *Public Participation in a Era of Governance: Lessons from Europe for Australia Local Government.* University of Technology, Sydney, Australian Centre of Excellence for Local Government, 2013.

FutureSight. *User Perspectives on Mobile Privacy.* GSMA, 2011.

Garry, T., F. Douma, and S. Simon. "Intelligent Transportation Systems: Personal Data Needs and Privacy Law." *Transportation Law Journal* 39 (2012): 97-164.

GSMA. *Accountability Framework for the implementation of the GSMA Privacy Design Guidelines for Mobile App Development.* Mobile and Privacy, GSM Association, 2013.

GSMA. *Privacy Design Guidelines for Mobile Application Development.* Mobile and Privacy, GSM Association, 2012.

Gubbi, J., R. Buyya, S. Marusic, and M. Palaniswami. "Internet of Things (IoT): A vision, architectural elements, and future directions." *Future Generation Computer Systems* (Elsevier) 29 (2013): 1645-1660.

Gubbi, J., S. Marusic, A. S. Rao, Y. W. Law, and M. Palaniswami. “A pilot study of urban noise monitoring architecture using wireless sensor networks.” *International Conference on Advances in Computing, Communications and Informatics.* 2013. 1047-1052.

He, Q., D. Wu, and P. Khosla. “The Quest for Personal Control over Mobile Location Privacy.” *IEEE Communications Magazine* 42, no. 5 (2004): 130-136.

Huang, K. L., and S. S. Kanhere. “A Privacy-Preserving Reputation System for Participatory Sensing.” *Proceedings of the 2012 IEEE 37th Conference on Local Computer Networks.* 2012. 10-18.

ICO. *Anonymisation: managing data protection risk code of practice.* Data Protection, UK: Information Commissioner's Office, 2012.

ICO. *Privacy by Design.* UK: Information Commissioner's Office, 2008.

ICO. *Privacy in Mobile Apps: Guidance for app developers.* UK: Information Commissioner's Office, 2013.

Ion, I., N. Sachdeva, P. Kumaraguru, and S. Capkun. “Home is Safer than the Cloud! Privacy Concerns for Consumer Cloud Storage.” *Proceedings of the Seventh Symposium on Usable Privacy and Security* . ACM, 2011. Article No. 13 .

Kang, J., K. Shilton, D. Estrin, J. Burke, and M. Hansen. “Self-Surveillance Privacy.” *Iowa Law Review* 97 (December 2012): 809-847.

Kanjo, E. “NoiseSPY: A Real-Time Mobile Phone Platform for Urban Noise Monitoring and Mapping.” *Mobile Networks and Applications* (Kluwer Academic Publishers) 15, no. 4 (August 2010): 562-574.

Kesan, J. P., C. M. Hayes, and M. N. Bashir. “Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency.” *70 Washingon & Lee Law Review* 341 (April 2013).

Kuznetsov, S., and E. Paulos. “Participatory Sensing in Public Spaces: Activating Urban Surfaces with Sensor Probes.” *Proceedings of the 8th ACM Conference on Designing Interactive Systems.* Aarhus: ACM, 2010. 21-30.

Longueville, B. D., and R. S. Smith. “OMG, from here, I can see the flames! : A use case of mining Location Based Social Networks to acquire spatio- temporal data on forest fires.” *Proceedings of the 2009 International Workshop on Location Based Social Networks.* 2009. 73-80.

Luo, T., and C.-K. Tham. “Fairness and Social Welfare in Incentivizing Partipatory Sensing.” *IEEE SECON.* 2012.

Maisonneuve, N., M. Stevens, M. E. Niessen, P. Hanappe, and L. Steels. “Citizen Noise Pollution Monitoring.” *The Proceedings of the 10th International Digital Government Research Conference.* 2009. 96-101.

Miedema, H. “Annoyance caused by environmental noise: Elements for evidence-based noise policies.” *Journal of Social Issues* 63, no. 1 (2007): 41-57.

Monaghan, D. *Data leaks in local government: where are the cracks in your system?* UK: Information Commissioner's Office, 2013.

OAIC. *Community attitudes to privacy survey.* Research Report, Office of the Australian Information Commissioner, Australian Government, 2013.

OAIC. *Data breach notification: a guide to handling personal information security breaches.* Office of the Australian Information Commissioner, Commonwealth of Australia, 2012.

OAIC. *Mobile Privacy: a better practice guide for mobile app developers.* Office of the Australian Information Commissioner, Commonwealth of Australia, 2013.

OAIC. *Privacy Impact Assessment Guide.* Office of the Australian Information Commissioner, Commonwealth of Australia, 2010.

Ostrom, E. “Crossing the Great Divide: Coproduction, Synergy, and Development.” Edited by M. McGinnis. *Polycentric Governance and Development. Readings from the Workshop in Political Theory and Policy Analysis.* Ann Arbor, MI: Univ. of Michigan Press, 1999.

Pachube. “Pachube data infrastructure.” (accessed 25-2-2011).

Palaniswami, M., S. Marusic, J. Gubbi, and Y. W. Law. *Noise Mapping: Designing an Urban Information Architecture to Record and Map Noise Pollution.* Feasibility Study, City of Melbourne, 2011.

Rana, R. K., C. T. Chou, S. S. Kanhere, N. Bulusu, and W. Hu. “Ear-Phone: An End-to-End Participatory Urban Noise Mapping System.” *IPSN'10.* Stockholm, 2010.

Reddy, S., D. Estrin, and M. Srivastava. “Recruitment Framework for Participatory Sensing Data Collections.” *LNCS* (Springer) 6030, no. Pervasive Computing (May 2010): 138-155.

Reddy, S., K. Shilton, J. Burke, D. Estrin, M. Hansen, and M. Srivastava. “Using Context Annotated Mobility Profiles to recruit Data Collectors in Participatory Sensing.” *LNCS* (Springer) 5561, no. Location and Context Awareness (2009): 52-69.

Santini, S., B. Ostermaier, and A. Vitaletti. “First experiences using wireless sensor networks for noise pollution monitoring.” *Proceedings of the 3rd ACM Workshop on Real-World Wireless Sensor Networks (REALWSN'08).* Glasgow: ACM, 2008. 61-66.

Shahabi, C., and A. Khoshgozaran. "Location Privacy in Geospatial Decision-Making." *LNCS* (Springer) 4777, no. Databases in Networked Information Systems (2007): 1-15.

Shilton, K. "Participatory Sensing: Building Empowering Surveillance." *Surveillance and Society* 8, no. 2 (2010): 131-150.

Shilton, K., and D. Estrin. *Ethical Issues in Participatory Sensing.* National Centre for Professional Research and Ethics, University of Illinois, CORE Issues in Professional and Research Ethics, 2012.

Shilton, K., J. Burke, D. Estrin, M. Hansen, and M. Srivastava. "Participatory Privacy in Urban Sensing." *Proc. International Workshop on Mobile Devices and Urban Sensing.* 2008. 1-7.

SmartSantander. 2013. http://www.smartsantander.eu/ (accessed January 2014).

Sobotova, L., J. Jurkovicova, Z. Stefanikova, L. Sevcikova, and L. Aghova. "Community response to environmental noise and the impact on cardiovascular risk score." *Science of the Total Environment* 408 (2010): 1264-1270.

Thierer, A. "The Pursuit of Privacy in a World Where Information Control is Failing." *Harvard Journal of Law & Public Policy* 36, no. 2 (2013): 410-455.

Vernez Moudon, A. "Real noise from the urban environment: How ambient community noise affects health and what can be done about it." *Am. J. Prev. Med.* 37, no. 2 (2009).

Wang, X., W. Cheng, P. Mohapatra, and T. Abdelzaher. "ARTSense: Anonymous Reputation and Trust in Participatory Sensing." *2013 Proceedings IEEE INFOCOM.* Turin, 2013. 2517 - 2525.

Widenoise. 2009. http://www.widetag.com/widenoise.

Wright, D., S. Gutwirth, M. Friedwald, P. de Hert, M. Langheinrich, and A. Moscibroda. "Privacy, trust and policy-making: Challenges and responses." *Computer Law and Security Review* (Elsevier) 25, no. 1 (2009): 69-83.

Yang, H. F., J. Zhang, and P. Roe. "Reputation modelling in Citizen Science for environmental acoustic data analysis." *Social Network Analysis and Mining* (Springer) 3, no. 3 (2012): 419-435.

THE UNIVERSITY OF MELBOURNE

IBES
Institute for a
Broadband-Enabled Society

Institute for a Broadband-Enabled Society
Level 4, Building 193
The University of Melbourne, Victoria 3010
e: contact@broadband.unimelb.edu.au
www.broadband.unimelb.edu.au