Public Sector Internet of Things Deployments: Value, Transparency, Risks and Challenges

[1]Naomi Jacobs*, [2]Peter Edwards, [3]Milan Markovic, [4]Caitlin D Cottrill, [5]Karen Salt

[1,2,3]School of Natural and Computing Sciences, University of Aberdeen, Aberdeen, UK
[4]School of Geosciences, University of Aberdeen, Aberdeen, UK
[5]School of Cultures, Languages and Area Studies, University of Nottingham, Nottingham, UK
naomi.jacobs@abdn.ac.uk

Abstract

Internet of Things (IoT) devices such as connected sensors are increasingly being used in the public sector, often deployed and collecting data in public spaces. While broadly perceived as beneficial by policy makers, such technology presents new challenges for governance. A theme commonly seen in the rhetoric surrounding public space IoT initiatives is empowerment. However, it is important to ask who is empowered and who benefits, and we must ensure that such technological interventions follow democratic principles and are trusted by citizens.

In this paper we describe work that utilises design fiction interventions in a community setting to explore questions of privacy, data management, risk and trust in relation to public space IoT deployments. Our findings suggest that agency, transparency and intent associated with IoT systems are key components that must be considered, particularly when multiple actors and stakeholders are involved.

We suggest that good governance requires consideration of these systems in their entirety, throughout the process, and in consultation with multiple stakeholders who are impacted, including the public. To achieve this effectively, we argue for transparency at the device and system level, which may require legislative change.

Keywords **–** Internet of Things; Accountability; Transparency; Trust

1 Introduction

The Internet of Things is a major growth area with significant economic and social implications (OECD, 2015). The term was coined by Kevin Ashton in the late 1990s to describe the collecting and sharing of supply chain data without direct human intervention (Ashton, 2009), and has come to be used more expansively to include a wide range of spatially-distributed devices that collect and transmit data. It has been claimed that there may be 20 billion such connected devices by 2020 (Gartner, 2017).

Increasingly, these technologies are not just being used in private contexts, but also public ones. Device deployments may be undertaken by public sector organisations to gather data for civic purposes, activities which are often grouped within the banner of the 'smart city' (Kitchin, 2014). Associated activities might include the installation of sensors and devices in shared public spaces, such as smart lighting, traffic management, or digitally controlled utility services. These spaces might also be host to devices deployed by individuals, industry or third sector organisations (for example the multi-partner 'Chicago Array of Things' project, led by an academic team, see Jacobs et al 2019). Public bodies might also seek to install or legislate for devices in semi-private and private spaces, such as temperature sensors in social housing (Davidson, 2018) or the UK's smart meter initiative in the energy sector (Department for Business, Energy & Industrial Strategy, 2016). This move towards technology as infrastructure requires new policy and regulation. The Internet of Things introduces new complexities of data governance, privacy and security, given the large volumes of data collected, involvement of multiple actors and stakeholders, the distribution across physical space, and questions of accountability at a variety of stages including procurement, deployment and management. For example, collecting large volumes of data has the potential to compromise privacy, particularly if personal data is included or can be inferred by linking a variety of data sources.

A theme commonly seen in the rhetoric surrounding public space Internet of Things (IoT) initiatives, particularly with regards to smart city programmes, is empowerment. Laced with articulations of enhanced democracy and openness, many IoT projects initiated by or carried out in the public sector are couched in language of increased efficiencies for overworked (often urban) infrastructure, economic benefits for citizens and users, the stimulation and vitalisation of new markets, and the positive social impact of digital-led innovations on the community (e.g. Gunashekar et al., 2016, Walport, 2014). It is, however, important to consider how this vision of digital opportunity and enrichment might be experienced by all social actors; not just those involved in leading these initiatives but those impacted, directly and indirectly, within the community and at all levels. In this paper, we report on work examining the governance at the national and local levels of public space IoT deployments and associated data capture. We explore whose visions contribute to developing these articulations of empowerment, as well as questions of value generated by such deployments and where this value might be located. We investigate how factors such as transparency and accountability can have a bearing on the rights of the public, and the trustworthiness of deployments which may have associated risks and challenges unforeseen by those governing and implementing them.

2 Context

Though the term 'smart city' is increasingly used by policymakers, industry and the media, many have expressed concern that the term is non-specific and of limited use. Angelidou (2014) notes that there remains no agreed definition of smart (or intelligent) cities. Kitchin suggests that it encompasses two distinct but related concepts; either the implementation of ubiquitous computing and digitally instrumented devices into the fabric of urban environments, or the broader development of a knowledge economy within a city region, a city "whose economy and governance is being driven by innovation, creativity and entrepreneurship, enacted by smart people" (Kitchen, 2014, p. 2).

This linkage between solutions that develop the knowledge economy and those that use IoT technology seems in some cases to be taken for granted. Many of those who discuss the implementation of smart cities, including policymakers, public representatives and technology providers, focus primarily on how digital and data-driven solutions can offer significant economic and social value. (e.g., Future Cities Catapult, 2017; Hill et al., 2016). This optimistic and somewhat reductionist approach suggests that being able to gather data will necessarily lead to solutions.

The EPSRC-funded TrustLens[1] project considers how these visions of digital opportunity and enrichment might be experienced by all social actors; not just those involved in leading the initiatives but those impacted, directly and indirectly, within the community where IoT solutions are deployed. If data collected via the initiatives are of value, who receives benefit, either financial or otherwise, from this collection? Who might be at risk? The ultimate goal of the project is to understand and enable trusted IoT ecosystems, from the perspective of those impacted by such systems.

In order to explore these questions, we have examined case studies of real deployments in the UK and worldwide. In addition to this, we have used ethnographic methods and design fiction methodology to undertake focussed participatory research with the Tillydrone community of Aberdeen. Tillydrone is known to have "a multiplicity of personal and social needs which exclude socially and economically disadvantaged residents from integration in the local community" (Lighthouse, 2018). This region has been designated as a regeneration area by the local council, and there have been multiple interventions to benefit citizens and address social needs. In our initial context-building work, we found that the trust relationship between the community and the local government is multifaceted, with some residents indicating that aspects of the relationship in the past, such as poor management of expectations, have led to mistrust.

2 Examining the Landscape

In our work examining the landscape of smart city funding and development, focusing particularly on the UK, we have observed that there is often pressure on local authorities to transform cities with technology and conform to positive rhetoric which assumes that benefit will automatically ensue. Technology solutions may be proposed by commercial providers or put out to tender by public bodies to solve a specific problem, endorsed by those who wish to improve services but are not necessarily familiar with the details of the technology and its privacy and security implications. Associated literature contains promises of efficiency savings and assumptions of upcoming ubiquity, without dwelling on the challenges of these implementations. While there is a multiplicity of smart city exemplars and demonstrators, we found that information sharing between regions and authorities is often limited,

[1] https://trustlens.org

with little communication of either best practice, or challenges that were encountered.

In implementing solutions that are designed for public benefit, it is important to also consider risks that may be encountered with widespread data collection in public spaces, which can also be seen as a form of surveillance (Vagle, 2016). Because some of these programmes are supplementing existing infrastructure, extensive public consultation is not always considered to be necessary. For example, while conducting ethnographic work in our community of interest, local residents queried the purpose of a new item of street furniture with no clear purpose or visible signage indicating who to contact for further information. This device-equipped street bollard uses sensors to monitor cycle and pedestrian traffic to inform transport planning, a function that would previously have been undertaken more sporadically through other means. This functionality facilitates transport management, but the installation occurred with limited transparency (a press release gave details of the initiative but was not widely distributed) precipitating trust issues within the community. While this particular deployment does not collect personal information, the generic device housing used could potentially have included a far greater range of sensors, without any visible difference.

Figure 1. Sensor enabled pedestrian and cycle tracker.

A particular question highlighted by our research is the complex nature of privacy and trust when data is collected in public spaces. It is not always possible to foresee all potential risks of data collection, particularly when multiple datasets exist and may be combined. In some cases it seems that the strategy of those initiating the deployments is to obtain as much data as possible, and decide what to use it for later. This seems to be in contravention of the ideals of data protection legislation such as the General Data Protection Regulation (GDPR)[2], which requires a clear purpose for data collection, but is complicated by the fact that much of this is environmental or situational data and considered non-personal.

3 Design Fiction

In a series of workshops with members of the Tillydrone community and local service providers, we began to interrogate questions of data privacy, data governance, risk and trust that may arise through the introduction of public space Internet of Things deployments. The first of these events was facilitated through our use of design fictions. These are 'diagetic prototypes' (Bosch, 2012): tangible objects which are created to depict fictional futures or alternate presents in which IoT deployments are deployed as part of public infrastructure.

Three sets of design fiction objects were developed based on the theme of waste and litter, identified by ethnographic work as a key concern of citizens in Tillydrone. Each of these acted as an 'entry point' to a worldbuilding scenario constructed by the project team. For example, one scenario envisioned the use of smart waste bins deployed by the local council in residential high-rise buildings which residents accessed through use of a contactless smart card. Materials presented to workshop participants included said card, information leaflets from the council which explained the function of the bins, and a letter to residents informing them of the roll-out process. What was not represented in these materials, despite being developed as part of the scenario, was the data flow (e.g. the nature of data collected and how it moved through various parts of the system) and governance (e.g. actors involved, decision making processes and intent). This included the detail that bins were purchased by the council from a commercial company, 'BinTech' who provided access to data produced by smart bins through a management dashboard but retained ownership. This additional information was presented in the form of data management maps at a later stage of the workshop.

By presenting materials representative of the usual levels of public communication around such deployments (e.g. press releases and informational leaflets) we aimed to examine the frequent lack of transparency evident in these systems, and the misunderstandings and assumptions which might therefore take place

[2] https://eugdpr.org/

Figure 2. Design fiction materials.

3.1 Findings

Through prompting the participants to consider more carefully the identity of the various actors involved, the nature of the data collected and the data management pathways, various potential risks emerged which had not previously been considered. Many participant concerns related to issues of transparency and agency. Although there was no immediate distrust of the deployments, or those putting them in place, there was concern over the idea that they may be happening without residents' knowledge or opportunity for input. This is linked to the idea that if such interventions occur without any prior notification or consultation, there is no opportunity for involvement in decision-making or control over the use of technology:

> *'It doesn't look like they asked anybody – the council are saying, we're doing this'*

> *'This has been pushed out to you rather than you opting to have it'*

> *'This is happening, and you have no choice'*

This theme of agency recurred, particularly given that some of the design fiction scenarios included devices deployed in public spaces, that gathered data from passers-by. The participants noted that it is not possible to opt out of such a system, particularly if deployed in a place that you move through frequently, or which, due to lack of appropriate notification materials such as signage, you are not aware of it at all.

> *'You'd probably have to opt out of everything'*

There were also particular concerns around data collection and management. When prompted to consider what data might be collected by such devices and deployments, participants began to question not only the specific details of data collected, but the intent behind it and who might be benefiting from its use.

> *'Are the local authority making money from selling data findings? To whom, and how is the data used and will it affect me… who's getting to find out about my habits?'*

It is important to note that the participants were not averse to the idea of selling data or profit being generated, as long as privacy was protected, ownership was considered, and those from whom the data were collected had knowledge of the process. One suggestion was that any revenue generated should be reinvested into the community.

> *'I would want them to tell me [if data was being sold]. So if you're doing this and I'm not getting any say in the matter…for your marketing and financial benefit, I want to know where that money's being spent.'*

> *'If they are benefiting from our personal data, it's not costing us anything to give it to them, but still. It's ours.'*

Participants were keen to know details of the deployments, their purpose, and what was happening to the resulting data collected through the use of such technology interventions. Key data management questions included knowing not only what data are being collected, but also why the deployment happened, who is collecting data, and who designed and manages the system as a whole. Additionally, some queries concerned the storage and security of the data, asking where it was being sent and stored, and who had ownership of it. Again, it was felt that if there was value in the data, this should be shared by the community, for example by giving the community access to data on public space usage in order to 'inform action and generate ideas' on how to better support the community.

Throughout the responses to the design fictions was a desire for transparency and communication to the public. It was reinforced that communication should be in a form that is accessible; using 'plain English' and preferably with support for questions to be answered.

> '*If this is being introduced in the community you need someone to come along to introduce it, to tell you its capabilities, answer all the questions you've got about it'*

Many participants were initially positive when introduced to these technologies, which were designed to solve community challenges such as littering and waste

management. However, the workshop questions prompted participants to question aspects such as privacy and value, and to consider more carefully the identity of the various actors involved, the nature of the data collected and, when revealed, the data management pathways. Through this process, they highlighted potential risks which had not previously been considered and were more cautious about their approval for such deployments.

4 Policy at multiple scales

Questions of transparency and data management are critical at various levels of governance, as illustrated by the discussions and findings above. Many different actors and stakeholders can be involved in public space IoT deployments, and it is useful to identify the different types of governance that might be relevant.

At the regional, national or super-national level, the use of smart technologies to support infrastructure is generally highly encouraged by policy. However, regulation must also be implemented to ensure that positive value does not come at the expense of the rights or safety of citizens. It is for this reason that the introduction of both legislation such as the GDPR and technology standards are important. However, governance and regulation should be ongoing processes rather than something implemented only once, particularly when IoT technologies are rapidly developing.

At the local level, there are considerations of governance when deployments are implemented. These can be initiated by a range of different actors including public sector bodies, commercial companies or ground-up, citizen led initiatives, and there may be different considerations of data management and privacy, surveillance and value depending on who these actors are and the motivation and intent of the deployment. It is important that these governance processes and actors are made clear to citizens, for example by publishing detailed but clear privacy and data ownership policies that inform the public about their rights.

At the system level, the technical specifications of the devices must similarly be transparent so that features of data collection, storage and transfer can be audited and made accountable. Design decisions must be taken that are conscious of potential risks, and efforts must be taken to mitigate them. Principles such as privacy by design and default that incorporate such values throughout the development process can form a key part of this. Organisations purchasing IoT sensor enabled devices must be able to determine what data are collected and shared, how this creates value, and who benefits.

By considering the system in its entirety at the outset, factoring in the position of and benefits to all stakeholders including citizens, public sector organisations and commercial technology providers, potential privacy and security risks can be identified in advance and appropriate choices made. Enforcing approaches such as privacy by design is not only good practice for protecting privacy, but encourages greater efficiency, and avoids preventable issues which may require costly fixes, for example, creating new software, hardware or policy.

5 Conclusion

If data collected via smart city and related public space IoT initiatives are of value, we must consider to whom it is of value; who receives benefit, either financial or otherwise, from its collection; and who might be at risk. Additional questions should be asked about whose rights are being enhanced, exploited or empowered and who is responsible when something goes wrong. When planning and implementing these deployments, actors involved must consider governance and policy at a variety of scales, and ask wider questions not only about data management, but also how decision making will affect multiple stakeholders who might be impacted. It is important to ask such questions at the start of the process and as data are being collected, and consider why data needs to be collected at all, rather than just collecting it because it is there with usefulness to be decided later. We have seen that assumptions can be made that connected technology is beneficial and helps people, with sometimes limited consideration of the associated risks, which may not become apparent until details of deployments are more closely interrogated.

A key outcome of this work is to highlight transparency and communication as critical; people need to be informed about deployments as they occur, and any associated risks. Deciding on the best way to include the public may not be straightforward, as information must be intelligible and comprehensible to a wide range of stakeholders. As a result of this work, we are developing tools to help different actors consider key aspects of public space IoT deployments. For example, prompting public sector bodies considering IoT solutions to be deliberative in their deployment and in their choice of how to manage the data generated. For individuals and communities, guidance will help in facilitating transparency and gaining access to information that they may otherwise not realise might be necessary.

Detailed policy guidelines and regulation should be used to prevent the use of inappropriate technology solutions which may entail risk to citizens or organisations. We also

highlight the need for transparency at the device and system level, and associated regulation to ensure this. Tenders to public organisations must ensure IoT solutions meet minimum standards which mitigate risks; for example, tracking data provenance to allow interrogation of data ownership and associated accountability. We hope to develop tools for encouraging mindfulness of these considerations during the planning, implementation, communication and evaluation processes; however, this must form part of a wider move towards an ethos of greater transparency.

It is important to emphasise that we do not suggest these technologies are not beneficial, nor that the public sector organisations who implement them are not sincere about improving the lives of citizens. However, in order for individuals and communities to be able to place trust in public sector IoT deployments, there must be transparency regarding the functionality, origins and risks entailed. The technologies must be properly implemented, and the significant challenges of privacy and governance, particularly with respect to data sharing, must be fully addressed. Meaningful accountability to and protection of the public must be incorporated into the new norms of technology as a facet of public service provision, so that data adds value and enhanced rights to all of society, rather than just a particular section of it.

Acknowledgements

This research was funded through the TrustLens project, supported by the award made by the RCUK Digital Economy programme to the University of Aberdeen; award reference: EP/N028074/1. We would like to thank the community of Tillydrone in Aberdeen for giving their time to this project.

References

Angelidou, M. (2014). Smart city policies: A spatial approach. *Cities*, 41, S3–S11.

Ashton, K. (2009). That 'internet of things' thing. RFID journal, 22(7), 97-114.

Bosch, T. (2012). Sci-Fi writer Bruce Sterling explains the intriguing new concept of Design Fiction. Slate, March, 2

Davidson, J. (2018) Renfrewshire uses internet of things technology to detect fuel poverty. *Holyrood* 24 January. Available online https://www.holyrood.com/articles/news/renfrewshire-uses-internet-things-technology-detect-fuel-poverty

Department for Business, Energy & Industrial Strategy, (2016). Smart Meters Implementation Programme 2016 progress update. UK Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/671929/Smart_Meters_2016_progress_update.pdf

Engelmore, R., and Morgan, A. eds. 1986. *Blackboard Systems.* Reading, Mass.: Addison-Wesley.

Future Cities Catapult. (2017). *Smart City Strategies: A Global Review 2017.* Future Cities Catapult. https://futurecities.catapult.org.uk/wp-content/uploads/2017/11/GRSCS-Final-Report.pdf

Gartner. (2017). *Leading the IoT: Gartner insights on how to lead in a connected world.* Gartner. https://gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

Gunashekar, S., Spisak, A., Dean, K., Ryan, N., Lepetit, L., & Cornish, P. (2016). Accelerating the Internet of Things in the UK. Santa Monica, Calif., and Cambridge, UK: Rand Corporation.

Hill, N., Gibson, G., Guidorzi, E., Amaral, S., Parlikad, A. K., & Jin, Y. (2016). *Scoping study into deriving transport benefits from big data and the Internet of Things in smart cities: Final report for Department of Transport*. Didcot, UK: Ricardo Energy & Environment.

Jacobs, N., Edwards, P., Cottrill, C., Salt, K. (2019, Forthcoming). Governance and Accountability in Internet of Things (IoT) Networks. In Oxford Handbook of Digital Technology and Society. Ed. Yates, S., & Rice, R. (Oxford University Press)

Kitchin, R. (2014). The real-time city? Big data and smart urbanism. GeoJournal, 79(1), 1-14.

OECD. (2015). *OECD Digital economy outlook 2015*. Paris: OECD Publishing. doi:http://dx.doi.org/10.1787/9789264232440-en

Vagle, J., 2016. The History, Means, and Effects of Structural Surveillance. U of Penn Law School, Public Law Research Paper, (16-3).

Walport, M. (2014). The Internet of Things: Making the most of the second digital revolution. A report by the UK Government Chief Scientific Adviser. The Government Office for Science. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf