*Data & Policy* (2020), 2: e11
doi:10.1017/dap.2020.11

**COMMENTARY**

# Who trusts in the smart city? Transparency, governance, and the Internet of Things

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

[1]School of Natural and Computing Sciences, University of Aberdeen, Aberdeen, United Kingdom
[2]School of Geosciences, University of Aberdeen, Aberdeen, United Kingdom
[3]School of Cultures, Languages and Area Studies, University of Nottingham, Nottingham, United Kingdom
*Corresponding author. Email: naomi.jacobs@lancaster.ac.uk

**Received:** 05 August 2019; **Revised:** 19 May 2020; **Accepted:** 02 June 2020

**Keywords:** accountability; Internet of Things; public space; transparency; trust

## 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. A theme commonly seen in the rhetoric surrounding public space IoT initiatives is empowerment, and these deployments are broadly perceived as beneficial by policy makers. However, such technology presents new governance challenges. 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 investigate how risk, transparency, and data governance require careful consideration in this domain, describing work which investigates how these combine to form components of trusted IoT ecosystems. This includes an overview of the landscape of public space IoT deployments, consideration of how they may often be subsumed in idealized smart city focused rhetoric, and discussion of how methodologies such as design fiction in community settings can uncover potential risks and concerns. Our findings suggest that agency, value and intent associated with IoT systems are key components that must be made transparent, particularly when multiple actors and stakeholders are involved. We suggest that good governance requires consideration of these systems in their entirety, throughout the full planning, implementation, and evaluation 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.

## Policy Significance Statement

Internet of Things (IoT) devices, which collect and share data, increasingly fill our environment. Ubiquitous data collection has great potential benefits, and these technologies frequently form a component of "smart city" programs favored by policymakers. However, important questions of privacy and data management must also be considered when introducing these technologies into public spaces. Many different groups may be affected by these deployments, and the needs of each must be considered. This article considers how transparency and effective governance can facilitate greater interrogation of public IoT deployments, key for developing more trustworthy IoT ecosystems. It highlights that policy and regulation are important at multiple scales; national, regional, and local, as well as at the level of the technology systems themselves.

## Introduction

The Internet of Things (IoT) 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 in public ones. Device deployments may be undertaken by public sector organizations to gather data for civic purposes, activities which are often discussed alongside rhetoric of the "smart city" (Kitchin, 2014). Examples of such activities and purposes might include the use of temperature, humidity, and $CO_2$ sensors within social housing (Davidson, 2018) to monitor aspects such as occupancy, damp, and potentially even complex issues such as fuel poverty. Sensors and devices may also be installed in shared public spaces such as smart lighting, traffic management, or digitally controlled utility services. Public sector deployments in these spaces join those undertaken by individuals, industry, third sector organizations, or a combination, for example, the multi-partner "Chicago Array of Things" project, led by an academic team (Jacobs et al., 2020). Public bodies might also seek to install or legislate for devices in private or semi-private spaces, such as the UK's smart meter initiative in the energy sector (Department for Business, Energy & Industrial Strategy, 2016). This move toward technology as infrastructure requires new policy and regulation. Instrumentation of public and shared environments using IoT technologies 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 (Urquhart et al., 2019).

A theme commonly linked with smart cities, and more specifically public space IoT initiatives, 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 vitalization of new markets, and the positive social impact of digital-led innovations on the community (e.g., Walport, 2014; Gunashekar et al., 2016). 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 commentary, we report on work examining the governance at the national and local levels of public space IoT deployments and associated data capture, and 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. Given that such data capture may have associated risks and challenges unforeseen by those governing and implementing it, we argue that factors such as transparency and accountability are crucial in protecting the rights of the public, and are important in ensuring the trustworthiness of IoT deployments. In exploring these questions, we build on work of the EPSRC-funded TrustLens[1] project, which 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. With such challenges exposed, we argue that designing and implementing such systems requires associated design of policy and governance that is informed by the needs of multiple stakeholders within these complex systems.

[1] https://trustlens.wordpress.com

**Examining the Landscape**

It is difficult to discuss public space IoT in an urban context without reference to the smart city. In our work, examining the landscape of public space IoT funding and development, focusing particularly on the United Kingdom, 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. In this sense, one answer to the question "who trusts in the smart city?" might be that local authorities trust in smart cities to provide promised solutions and benefits. 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. However, procurers are not necessarily familiar with the details of the technology and its privacy and security implications. Materials produced by technology providers, as well as public sector strategy documents, often contain 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, with little communication of either best practice, or challenges that were encountered. This concurs with the "self-congratulatory" trend described by Hollands (2008).

Though the smart city term is increasingly used by policymakers, industry and the media, many have expressed concern that it is nonspecific and of limited use (Hollands, 2008; Angelidou, 2014; Kitchin, 2014). Angelidou notes that there remains no agreed definition of smart (or intelligent) cities. Kitchin (2014), p. 2 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". 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., Hill et al., 2016; Future Cities Catapult, 2017). This optimistic and somewhat reductionist approach suggests that being able to gather data will necessarily lead to solutions (Hollands, 2015). However, this is not necessarily the case and in this sense unconditional trust in the positive consequences of smart cities is perhaps misplaced.

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. However, this is complicated by the fact that much of this is environmental or situational data and considered nonpersonal.

In implementing solutions that are designed for public benefit, it is important to 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 programs 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).

[2] https://eugdpr.org/

**Speculative Methods for Understanding Opportunities and Risk**

The bollard described above caused concern in our community of interest, those resident in the Tillydrone region 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. Such marginalized communities are not always beneficiaries from new technology implementation (Gurstein, 2011). When asking "who trusts in the smart city," the types of people who come to mind as being within the smart city ecosystem (and therefore having varied levels of trust) may not be inclusive of those who live in places such as Tillydrone. 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. It may be challenging for such communities to have trust in IoT technologies implemented as part of transforming their environment to a smart city when there is not an assumption of trust in public service provision before the city becomes smart.

The issue in the case of the bollard was not the deployment itself, which had a clear benefit and benign purpose, but the lack of transparency, which meant that the public did not have the information necessary to ensure trust. In order to properly interrogate IoT systems which are being deployed in public spaces, it is important for these systems to be transparent. This involves both transparency of the governance processes that has led to their implementation, and for the systems and devices within them to have transparency of function; that it is possible and easy to find out and understand what the devices are intended to do, what they actually do and where accountability lies.

As previously mentioned, there are significant challenges to considering the future implications of such novel systems and solutions that involve a wide range of stakeholders and contexts. We suggest that

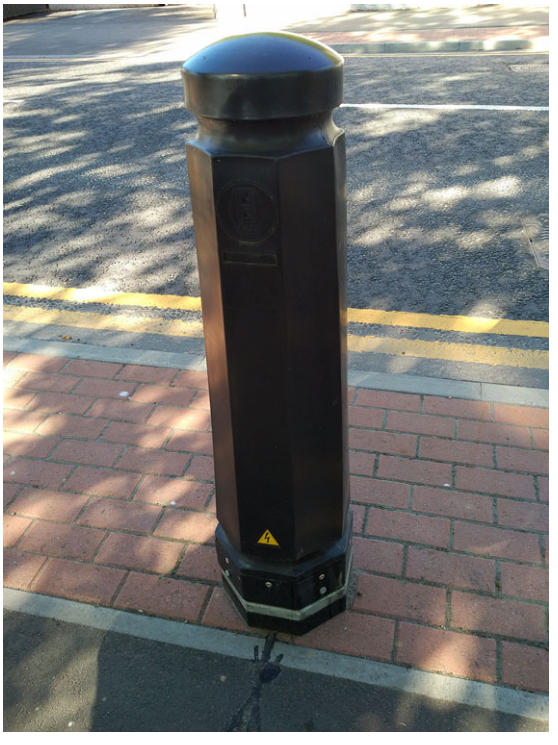

***Figure 1.*** *Sensor enabled pedestrian and cycle tracker.*

when considering the design and deployment of such systems it is necessary to incorporate new speculative methods which enable the development of new understanding. This can thus feed into the design of appropriate policy and can keep pace with fast-moving new solutions. In a series of workshops with members of the Tillydrone community and local service providers, we used a design fiction methodology to interrogate questions on topics such as data privacy, data governance, risk, and trust that may arise through the introduction of public space IoT deployments. Design fiction involves the design of "diagetic prototypes" (Bosch, 2012): tangible objects which are created to depict fictional futures or alternate presents. In this case, the design fictions represented a version of Tillydrone in which IoT deployments are being deployed as part of public infrastructure, specifically three different scenarios of waste management using distributed IoT solutions with associated design fiction prototype objects. 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 would access 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 (i.e., 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, for example, the detail that bins were purchased by the council from a commercial company, "BinTech," who provided access to resulting data via 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, and was of some surprise to the participants who often found it did not match their initial assumptions.

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 Figure 2.

## Transparency and Agency

When initially presenting our scenarios and objects to the participants, we found a range of attitudes towards these technological solutions. 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

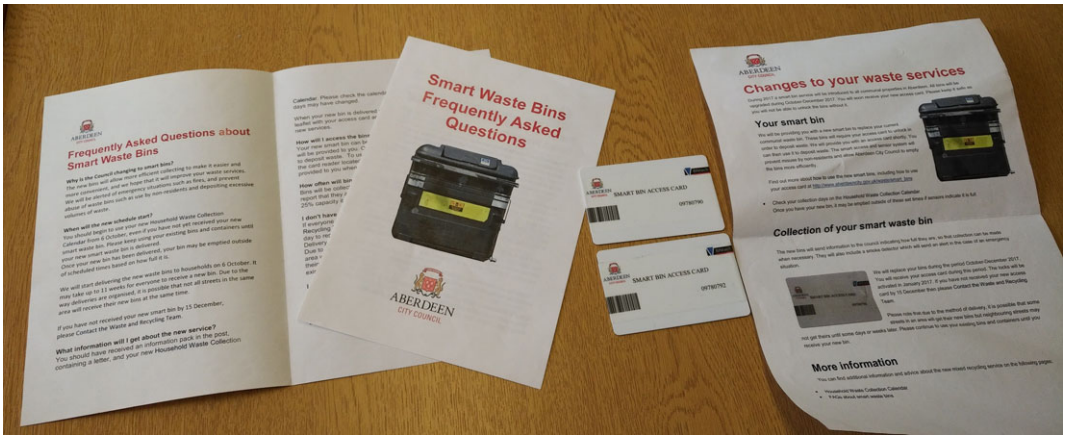


***Figure 2.*** *Design fiction materials.*

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. By talking through aspects of the systems and receiving prompts regarding aspects such as data management and governance, various potential risks emerged which they had not considered at the outset. 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. One participant commented: "*It doesn't look like they asked anybody—the council are saying, we're doing this.*" No opportunities were presented for opting out of a deployment that could potentially have implications for the lives of residents.

This notion of agency was recurrent, particularly given that some of the design fiction scenarios included devices that gathered data from passers-by and would be deployed in public spaces. The participants noted that it may not be possible to opt out of such a system, particularly if deployed in a place that you move through frequently, or in which you are not aware of its presence at all due to lack of appropriate notification materials such as signage. Participants also raised concerns relating to 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 migh benefit from its use. Financial benefit from the selling of data was not seen as necessarily detrimental as long as privacy was protected, but ownership was a topic of discussion, for example, with one participant suggesting that any revenue generated should be reinvested into the community.

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, participants demonstrated a desire for transparency and communication to the public. Furthermore, they reinforced the view 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"*

## Policy at Multiple Scales

The findings above demonstrate that transparency is desirable for those who may be encountering IoT deployments in their environments. To provide transparency requires that considerations of privacy and data management are understood by those implementing the systems. This also enables transparency of processes between regional programs to share learning and avoid repetition of costly mistakes.

At the local level, deployments can be initiated by a range of different actors, including public sector bodies, commercial companies, or ground-up citizen-led initiatives. 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 transparent governance processes are in place and citizens can identify the actors involved, 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. Organizations purchasing IoT sensor enabled devices must be able to both determine and communicate 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 organizations, 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, avoiding preventable issues which may require costly fixes, for example, creating new software, hardware, or policy.

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 legislation such as the GDPR and technology standards are important; however, we argue that such systems and their processes must also be transparent and consider the needs of multiple stakeholders at various levels. It is important that governance and regulation should be ongoing processes rather than something implemented only once, particularly when IoT technologies are rapidly developing.

## Conclusion

At the regional, national, or super-national level, we have observed that the use of smart technologies to support infrastructure is generally perceived in ideologically positive terms (Hollands, 2015) and is highly encouraged by policy (Jacobs et al., 2020). However, 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 regarding 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. Furthermore, it is also important to 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 but with sometimes limited consideration of the associated risks, some of which may not become apparent until details of deployments are more closely interrogated.

In this work, we highlight transparency and communication as critical; in order to be able to trust in the smart city, 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. Through the work of the TrustLens project we are developing tools to help different actors consider key aspects of public space IoT deployments. For example, a digital and physical "card deck" presents questions covering multiple aspects of the deployment process, and asks different stakeholders to consider whether they have answers immediately available, or need to conduct further scoping and research. Such tools encourage public sector bodies who are considering IoT solutions to be deliberative in their deployment and in their choice of how to manage the data generated. Guidance for individuals and communities will aid in the facilitation of transparency and assist in gaining access to information that they may otherwise not realize might be necessary.

We also recommend that detailed policy guidelines and regulation should be used to prevent the use of inappropriate technology solutions which may entail risk to citizens or organizations. There is a need for transparency at the device and system level, and associated regulation to ensure this. Tenders to public organizations must ensure IoT solutions meet minimum standards which mitigate risks; for example, tracking data provenance to allow interrogation of data ownership and associated accountability. Tools such as those described above aim to encourage mindfulness of these considerations during the planning,

implementation, communication, and evaluation processes; however, this must form part of a wider move toward an ethos of greater transparency.

It is important to emphasize that we do not suggest IoT technologies associated with smart city rhetoric are not beneficial, nor that the public sector organizations 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 and ownership, 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, in order for data to add value and enhance the rights to all of society, rather than just a particular section of it.

**Acknowledgments.** We would like to thank the community of Tillydrone in Aberdeen for giving their time to this project. A version of this work was previously made available for the Data for Policy conference 2019 (Jacobs et al., 2019).

**Funding Statement.** This research was funded through the TrustLens project, supported by the award made by the RCUK Digital Economy program to the University of Aberdeen; award reference: EP/N028074/1. The funder had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

**Competing Interest.** The authors declare no competing interests exist.

**Authorship Contributions.** Conceptualization, N.J., K.S., and C.D.C.; Investigation, N.J., C.D.C., M.M., and P.E.; Writing-original draft, N.J.; Writing-review & editing, N.J., P.E., C.D.C., M.M., and K.S.; Funding acquisition, P.E., C.D.C., and K.S.

**Data Availability Statement.** The qualitative data collected as part of this research is not openly available, but may be accessed for research purposes by contacting the authors. This is for ethical reasons, due to the nature of the consent given by participants who contributed to the research.

## 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*, 2 March 2012. Available at https://slate.com/technology/2012/03/bruce-sterling-on-design-fictions.html. (accessed 13 June 2018).

**Davidson J** (2018) Renfrewshire uses internet of things technology to detect fuel poverty. *Holyrood*, 24 January. Available at https://www.holyrood.com/articles/news/renfrewshire-uses-internet-things-technology-detect-fuel-poverty. (accessed 13 June 2018).

**Department for Business, Energy & Industrial Strategy** (2016) Smart Meters Implementation Programme 2016 progress update. *UK Government.* Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/671929/Smart_Meters_2016_progress_update.pdf. (accessed 13 June 2018).

**Future Cities Catapult** (2017) Smart city strategies: A global review 2017. *Future Cities Catapult.* Available at 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.* Available at https://gartner.com/imagesrv/books/iot/iotEbook_digital.pdf. (accessed 13 June 2018).

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

**Gurstein MB** (2011) Open data: Empowering the empowered or effective data use for everyone? *First Monday 16*(2).

**Hill N**, **Gibson G**, **Guidorzi E**, **Amaral S**, **Parlikad AK and 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*.

**Hollands RG** (2008) Will the real smart city please stand up? *City 12*(3), 303–320.

**Hollands RG** (2015) Critical interventions into the corporate smart city. *Cambridge Journal of Regions, Economy and Society 8*(1), 61–77.

**Jacobs N**, **Edwards P**, **Cottrill C**, **Salt K** (2020) Governance and accountability in internet of things (IoT) networks. In Yates S and Rice R (eds), *Oxford Handbook of Digital Technology and Society*. Oxford, UK: Oxford University Press.

**Jacobs N**, **Edwards P**, **Markovic M**, **Cottrill CD and Salt K** (2019) Public sector internet of things deployments: Value, transparency, risks and challenges. *Zenodo.* Available at http://doi.org/10.5281/zenodo.2713118. (accessed 19 June 2020).

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

**Lighthouse** (2018). About us. Lighthouse. https://lighthouse-abdn.org.uk/about-us/

**OECD** (2015) *OECD Digital Economy Outlook 2015*. Paris, France: OECD Publishing. http://dx.doi.org/10.1787/9789264232440-en

**Urquhart L**, **Lodge T and Crabtree A** (2019) Demonstrably doing accountability in the Internet of Things. *International Journal of Law and Information Technology 27*(1), 1–27. https://doi.org/10.1093/ijlit/eay015.

**Vagle J** (2016) The history, means, and effects of structural surveillance. University 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. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf. (accessed 1 June 2018).

**Cite this article:** Jacobs, N. Edwards, P. Markovic, M. Cottrill, C. D. and Salt, K. 2020. Who trusts in the smart city? Transparency, governance, and the Internet of Things. *Data & Policy*, 2: e11. doi:10.1017/dap.2020.11