Research Article

Perspectives on citizen data privacy in a smart city – An empirical case study

Evie Lucas
Manchester Metropolitan University, UK

Seamus Simpson ⓘ
University of Salford, UK

Abstract

Digitisation is arguably an inevitable feature of contemporary urban development, yet privacy issues arising from the mass data collection, transmission and processing it entails continue to be a poorly understood and contentious issue for people living in cities. This article uses a case study approach to provide new evidence of the detailed perspectives of citizens and policy makers on data privacy in rapidly digitising urban environments, with a focus on one of the UK's most prominent smart cities: Manchester. It adds to the literature on smart cities through the application of complementary scholarship from two areas – trust and participation – in order to analyse comparatively citizens' views and concerns on data gathering activity in their city with efforts of policy makers to in-corporate data privacy matters in their digital city planning. The article finds a clear – but reparable – data privacy disconnect between people and digital policy makers and explores how citizen data privacy concerns may be addressed through a lens of trust and participation.

Keywords

Citizens, data privacy, smart cites

Introduction

As rapid urban population growth, combined with climate change, place an increasing burden on environmental and public resources, the deployment of digital technologies and communications networks has been posited as the panacea to increase the resilience and sustainability of cities. Cities are expected to be at the forefront of using 'smart' tools to predict and respond to future emergencies – a 2020 OECD report claimed that 'COVID-19 accelerated the shift towards a new

Corresponding author:
Seamus Simpson, School of Arts, Media and Creative Technology, University of Salford, MediaCityUK, Salford, UK.
Email: s.simpson@salford.ac.uk

urban paradigm…[of]… inclusive, green and smart cities' (OECD, 2020: 3), and GlobalData research suggested that spending on global smart cities will grow from $221.1bn in 2019 to $442.6bn in 2025 (Global Data, 2022). Smart cities embody convergent media environments, since they deploy electronic devices to collect and process data about the physical world in real time; transmit these data through communication networks; and process and use the results of data analysis to plan and provide applications to users to improve their living experiences and standards. No two smart cities are the same, but they all incorporate some applications that monitor and leverage energy consumption, air quality and pollution levels, traffic and congestion patterns, public health and other aspects of daily life (Zhang et al., 2017) – applications which require, generate and transmit very large quantities of data (Van Zoonen, 2016).

The concept of a smart city can be traced back to the 1980s, though it is only in recent years that academic interest in the topic has intensified, where according to Sharifi et al. (2021: 6) the number of articles published between 2018 and 2021 was greater than the cumulative total published in the previous 17 years. Amongst this body of work, considerable scholarly attention has been paid to the construction and development of smart cities from a techno-infrastructural perspective. Rather differently and in part as a consequence, more critical, citizen-focused academic work has problematised the position and role of citizens in smart city developments (Calzada, 2021; Cardullo and Kitchen, 2019). Part of this scholarship has explored the consequences of smart city development for the data privacy of its citizens, highlighting control and intrusion, data commodification, de-personalisation, and opaqueness as an unpleasant roster of the potential consequences of smart city roll out (Kitchin 2014; 2016). This article builds on such scholarship through generation and analysis of detailed evidence of the experiences of both citizens and policy makers on data privacy in smart cities in order to deepen our understanding of its significance and implications. The article achieves its contribution through the creation of a conceptual lens to assist in its analysis of smart city data privacy issues by drawing together and applying separate academic work on trust in government (Jennings et al., 2021) and participation in smart cities (Cardullo and Kitchen 2019). The article outlines briefly how Manchester, our case study, exemplifies long-standing efforts by a city to introduce information and communications technologies for economic and social gain, something which has received some limited coverage in the literature to this point (see Caird, 2018; Cowley and Capriotti, 2019). This creates a context for a detailed exploration in the article of the experiences, viewpoints and preferences of citizens and civic policy makers on data privacy issues and, in so doing, the article illustrates how even well-established smart cities face major challenges in addressing citizen concerns about privacy. This evidence leads the article to consider, in its conclusion, measures which might be introduced to address the concerns identified in the empirical evidence presented in the article through understandings of (mis)trust and smart city participation. Through drawing on conceptualisations of 'mistrust' as an open, fluid and socio-politically valuable concept, with its core features of vigilance, caution and questioning, the article argues that, if addressed appropriately by policy makers in their consideration of data privacy matters, it holds the potential to deepen the level of citizen participation in smart cities.

The smart city

The concept of a smart city and its potential ways of functioning in practical terms are complex and multifaceted, so it is perhaps unsurprising that there is little agreement on a precise definition of the term, with different authors' definitions reflecting the emphasis that each one gives to information and communication technologies (ICT), the creative economy, human experiences, and well-being

and sustainability (see Albino et al., 2015; Lara et al., 2016, for comprehensive analyses of the different definitions and dimensions of smart cities).

Pali and Schuilenburg (2020) argue that the idea of being smart has been associated with a variety of terms related to creativity, intelligence, virtuality, the digital and interconnection, all underpinned by developments in information technology hardware and software, and data processing. Martin et al. (2018) note three core visions of the smart city underpinned by ideas of digitality, entrepreneurship and sustainability. Sadowski and Pasquale (2015) acknowledge the flexibility of the term, but emphasise the relationship between technology and politics in the evolution of digital urban environments. For the purposes of this study, a smart city is defined broadly as one that uses digital technologies in a co-ordinated manner with the goal of improving the quality of life of its citizens now and in the future. It is a definition that views the diffusion of ICT as the means to a human-centred end: enhancing people's quality of life by enabling them to live in sustainable, innovative, empowered and connected communities. This is consistent with various academic definitions (e.g. Eger, 2009; Guan, 2012; Bakici et al., 2012, cited in Albino, 2015) in its emphasis on the people and communities within a city.

A key technological development in the emergence of the smart city is the Internet of Things (IoT), where 'information and communication systems are invisibly embedded in the environment around us' and where internet-enabled, smart devices undertake regular, sustained communication with each other using sensors and actuators (Gubbi et al., 2013: 1645). IoT devices are able to recognise, locate, track, monitor and manage, generating real time data streams which are germane to the functioning of smart cities.

Smart cities and data privacy

The widespread collection, processing and use of big data by private and public actors in smart cities has implications for privacy. Privacy is a complex, multifaceted and interdisciplinary concept that is 'fundamentally important – both for individuals and for societies' (Bräunlich et al., 2021). For the purposes of this article, we focus on privacy as the right of individuals to 'control information about them and decide when, how and to what extent information is communicated to others' (Westin, 1967: 7) – a right that is under severe pressure (Knijnenburg et al., 2022). Critical scholarly work on smart cities from a data privacy perspective has raised the concern that they can become new centres of surveillance and control (De Zwart et al., 2014; Hollands, 2008). Foucault (1977) illuminated discipline-inducing effects of 'panoptic' surveillance across a wide set of social contexts. Surveillance has become broader in the digital age, with observational and predictive motivations guiding its data gathering and analysis. Nissenbaum (2004) highlighted the link between public surveillance, information technology and privacy. Surveillance can undermine trust through interfering with 'the sense of privacy and urban anonymity that has defined urban life over the past century' (Finch and Tene, 2013: 1582). The idea of growing surveillance (Bogard, 1996) has been associated with the growth of surveillance both by governmental actors and commercial entities, particularly relevant to smart cities which are noteworthy for operating through a variety of public/private partnerships where data is shared across the public/private divide. Utz and Krämer (2009) provide evidence of a privacy paradox, where growing citizen concern over privacy is not matched by action in service of securing it and, relatedly, a transparency paradox (Nissenbaum, 2019), where the provision of detail to users about data privacy procedures can result in a reduction of understanding about them (Hilden, 2019). Pali and Schuilenburg (2020) highlight newer modes of control in smart cities, which they argue link embedded surveillance with neoliberal ideas and

practices. Relatedly, Kitchin (2019) argues that smart city developments are led by an urban political and technical elite, where initiatives are often imposed on citizens with little or no consultation.

Smart cities, trust and participation

Whilst surveillance within a smart city can be aimed at improving urban life (Ziosi et al., 2022) it can also lead to the undermining of civic trust. Thomas et al. (2016) note that the term smart city can be difficult to understand and relate to for citizens, exemplified by the remoteness and lack of visibility of many of the technological objects and processes constituting its fabric and function. While living in smart cities has been associated with empowerment (Shelton and Ladato, 2019), due to its often invisible infrastructure, people can become involuntary data sources with a 'loss of data sovereignty' (Eckhoff and Wagner, 2017) making opting out difficult and undermining trust. Beldad et al. (2011: 47) analysed Dutch users' trust in the processing and use of personal data by government organisations, finding that 'confidence in online privacy statements is a very important determinant of their trust in government organisations in terms of how they use and process citizens' personal data'. More recently, drawing on academic work which has established the greater willingness of people to share temporarily data with public, rather than private, organisations Trein and Varaone (2023) explored the conditions under which citizens are willing for their personal data to be used in national policy making in Switzerland, working with the idea (after Rousseau et al., 1998) of trust as a state of accepted vulnerability in the expectation of a positive outcome. Their key finding is that people 'are more likely to share data if they believe that the policy problem the State seeks to solve is important to them and if they trust their government' (Trein and Varone, 2023: 3). Kennedy et al. (2020) have found that people are concerned about, and find ways to defy, data practices in their everyday lives. Marwick and Hargittai (2019) focus on factors explaining young people's willingness to share information online with institutions. They draw on the idea – and find evidence – of a privacy calculus which assumes that individuals undertake a rational evaluation of imparting information. They used the focus group method 'allowing participants to define privacy and explore nuance and context in their experiences' (p.1699) and found that people 'are incentivised by financial benefits, health benefits, convenience, and necessity…[and]…are disincentivized by lack of trust, fears of online harassment, and fears of discrimination…and evaluate the information type, context, and institution requesting the information'.

Recent work by Jennings et al. (2021: 1176) on trust has argued that 'trust or confidence in government is seen as a key ingredient for good governance and its absence is viewed as likely to undermine governing capacity'. They posit an extension of the idea of trust into what is called the 'trust family', comprising the three elements of trust, mistrust and distrust. Marien and Hooghe (2011: 267) note that whilst a dominant perspective is that 'low levels of political trust should be a major reason for concern', an alternative perspective holds that 'low levels of political trust might offer an opportunity for the further development of democratic political systems as the rise of a new generation of "critical citizens" might force…decision makers to react in a more responsive manner'. Lenard (2007: 313) elaborates on this idea by contending that 'arguments that make distrust the central element of democracy fail…alongside trust we need to adopt a kind of vigilance, an attitude that is motivated by mistrust, in order to maintain a healthy democracy'. Here, the idea of mistrust refers specifically to doubt and scepticism, unlike the 'settled belief that the other is untrustworthy' entailed in outright distrust (Citrin and Stoker, 2018: 50). Mistrust can manifest as 'vigilance in judging components of the political system', being cautious, watchful and questioning and 'making effort to be informed, alert, on standby to act' (Jennings et al., 2021: 1177, Table 1). Importantly, a 'lack of trust is not the same as positively believing the government is acting against

Table 1. Demographic characteristics of workshop participants.

Demographic characteristics	Percentage
Gender (*n* = 30)	
Female	56.7
Male	40
Non-binary	3.3
Age (n = 30)	
18–30	53.3
31–40	20
41–50	6.7
51–60	10
61–70	3.3
71–80	3.3
80+	3.3
Academic qualifications (*n* = 27)	
High school diploma or equivalent	18.5
BA/BSc degree	40.7
Master's degree	33.3
Doctorate	3.7
Other	3.7
Ethnicity (*n* = 30)	
White	53.3
Black	16.7
Asian	30

your interests' (p.1187). More specifically, mistrust 'is more likely to translate into ambivalence about others' trustworthiness rather than into a perception that they cannot be trusted at all' (Lenard, 2008: 318).

When this is combined with the understanding that 'trust is a resource enabling government action' (Citrin and Stoker, 2018: 62), the idea of how to harness a situation of mistrust and move it in the direction of trust becomes important. Mistrust can be viewed a positive phenomenon for two reasons. First, it can create the conditions for a residual questioning of the motives of policy makers. Second, rather differently, it can serve as a healthy pre-condition for the establishment of trust through processes of dialogue and purposeful engagement between public policy makers and citizenry.

The idea of mistrust as a route to progressive public policy change and enriched citizen experience can be usefully complemented by exploration of academic work on citizen participation. Cardullo and Kitchen (2019) explore the idea of citizen involvement in the smart city specifically by extending earlier work of Arnstein (1959) on citizen participation into what they term the 'scaffold of smart city participation'. Some of the elements of the scaffold are relevant for matters of data privacy. In their consideration of 'non participation', they highlight how citizens can become little more than data points with no agency to engage with the generated data. Under a neoliberal discourse of efficiency and environmental sustainability, people are thus 'steered and controlled', whose data can be mined, combined, traded and used for future planning purposes (p6.). They also note that new administrative layers and practices, not least related to public-private collaborations,

create remote and inaccessible arrangements which 'dissipate a transparent and democratic process'. Another part of their participation scaffold concerns tokenism, which can take various forms, the most cursory being one-way informing of citizens (where they can access open data), through to more involved consultation and placation. Whilst the latter can work to keep 'civic paternalism in check' (p.8), the authors point out that the data generated from such exercises can be packaged and sold commercially. A more citizen-involved part of the scaffold concerns: 'citizen power', involving co-creation; 'partnership', comprising shared planning and decision making on projects; and 'citizen control', where people are in full control of the policy and managerial aspects of a program. Kitchen and Cardullo find little or no evidence of such kinds of participation, instead concluding that citizens contribute to the reproduction of neoliberal smart city approaches where they 'are encouraged to help provide solutions to practical issues…but not to challenge or replace the fundamental political rationalities shaping an issue or plan' (p12). This pessimistic conclusion is also reached by Breurer and Pierson (2021) in their exploration of data protection in smart cities from the classic citizen-focused 'right to the city' perspective articulated by Lefebvre (1968) and drawing on more recent ideas that 'smart city technologies can – and should – enhance inclusion of citizens, public participation and civic engagement'. Arguing in favour of a participatory approach for people in smart city development contexts along the lines of the 'right to city' idea, they too, however, find a 'kind of public participation a long way removed from citizens having the right to the city' (p.807). These valuable insights can be used to understand the detailed perspectives of citizens and policy makers on data privacy in smart cities. What are the experiences and perspectives of citizens living in a well-established smart city on privacy related to data collection practices? How does this compare to the experiences and perspectives of policy makers and what can be done to reconcile differences and create a more citizen-considerate smart city environment in respect of data privacy? To what extent does mistrust among citizens in respect of data privacy practices exist and how can this be harnessed to increase levels of participation in smart cities?

Manchester as a smart city

Manchester exemplifies a significant number of the ideas and practices associated with the smart city. Since the early to mid 1980s, there is evidence of a series of often highly successful attempts to harness the potential of information and communications technologies for economic renewal and growth. This – now recognisably pioneering – work led to initiatives, such as Manchester Host (1991), electronic village halls (1992), and the Manchester Community Information Network (1994), which were launched prior to the popularisation of the Internet through the World Wide Web (WWW). The creation of a telematics strategy in 1997 followed, as well as projects to connect the unconnected, such as Eastserve (Carter, 2019). A feature of Manchester's digital development was its utilisation of the European Union (EU) as a reference point and funding source: Manchester became a leading player in the EU Eurocities initiative, where issues of digital development were prominently positioned. Cowley and Capriotto (2019: 430) argue that Manchester provides an example of a city that has deployed experimental local practices at 'the "cutting edge" of smart urbanism in the UK' though without 'clear linearity (either narrated or practised) between formal strategies, plans and activities' (p.435). Caird (2018: 176) in a comparative study of a number of UK smart cities, including Manchester, argued for the creation of more effective management 'to support reporting through the wider community of partnerships of *all* the organisations responsible for the delivery of city strategies and plans around smart city outcomes, across the government, industry, university and citizen groups' (emphasis in original).

By 2008, Manchester had launched its own digital strategy and its deepening engagement with research at the EU level on the digital led to discussions on the IoT and its relationship to citizen based web services (Carter, 2019) and, by 2010, Manchester chairing the EU funded European Connected Smart Cities network. At the core of Manchester's approach was the 'Smart Citizens in Smart Cities' idea, drawing on a four level social capital model which sought to utilise digital technologies to create a sense of belonging for citizens, to improve access to technologies and services for social engagement, to engage diverse communities with digital technologies, and to use digital technologies to breakdown workplace and societal barriers and promote social cohesion. The development of a Digital Strategy became a core concern of the Greater Manchester Combined Authority (GMCA), formed in 2011. The *Greater Manchester Digital Blueprint* (2020-23) established a number of priorities, several of which point up the importance of privacy issues. Priority 1, 'Empowering People', states that 'people should have absolute confidence in what happens to their data'. Priority 2 'Enabling Innovative Public Services' declares the goal to 'use data responsibly and effectively'. Priority 5 sets the goal of establishing the city region as a UK and European centre for cybersecurity and digital ethics.

In 2015, Manchester was selected out of 34 applicant cities across the UK for a £10 million government award to fund a two-year smart city demonstrator (gov.uk, n.d). The CityVerve project was a consortium led by Manchester City Council that brought together 20 public and private organisations with the aim of using Internet of Things technology to create a blueprint for smart cities in the UK. It was a widely publicised project that established Manchester as a leading smart city.

In March 2022, Manchester City Council (a part of the GMCA) launched its latest digital strategy. Two of the four key themes of the strategy are 'smart people' related to digital skills acquisition and 'digital places', which focuses on network access and digital infrastructure in connected digital neighbourhoods, as well as using data to ensure effective delivery of digital services (Manchester City Council, 2020). The Digital Places theme has important implications for privacy matters. The strategy asserts that information should be 'protected and treated with care, especially in terms of data quality, ethics and security'. The strategy draws on the Eindhoven Principles of data ethics and social responsibility whose first principle is 'Privacy First'. It asserts that 'Digital places should ensure that a similar set of principles are adopted to ensure that digital and technology are deployed and used in an ethical and responsible way' (Manchester Digital Strategy, 2021-2026: 12). In its strategy, the Council asserts that 'we also understand the importance of ethics, sustainability and security when handling data, and that we need to be proactive in ensuring that systems and processes are in place to effectively manage information' (Manchester Digital Strategy, 2021-2026: 14).

Against this backdrop, after a brief section explaining its methodological approach, the article proceeds to explore in detail citizen perspectives on – and experiences of – data privacy and compares them to those of Manchester smart city policy makers.

Methodology

The research underpinning the article used a case study strategy (Yin, 2012) to collect evidence from different sources and drew together data in order to gain knowledge of, and account for, understandings of citizen privacy in a smart city (Manchester). Data was collected using workshops, an online questionnaire and semi-structured interviews, in addition to relevant primary source documents. Although statistical generalisation is neither possible nor desirable in this case, a rigorously conducted case study can help a researcher gain a deeper understanding of a phenomenon and allow

analytic generalisation (Yin, 2012). Our aim is not to develop predictive theories but to provide a nuanced view of the reality of data privacy for citizen and policy actors in a smart city and, as such, and in line with Flyvberg (2006: 223), 'the case study is especially well suited' to offer 'concrete, context-dependent knowledge'.

A set of semi-structured interviews with digital city policy makers was undertaken and analysed thematically to establish perspectives on matters of citizen data privacy. At the same time, a questionnaire was used to identify attitudes to data collection and privacy in smart cities among Greater Manchester citizens. The citizen voice is important since 'surveys and interviews that reflect citizens' opinions need to be used to implement smart city policies that citizens can feel' (Myeong et al., 2022: 13). Questionnaire participants were recruited from the diverse communities that make up Greater Manchester, with posts appearing on social media, but also on notice boards in local churches, libraries, train stations and community centres. As a result, although the survey sample is relatively small, its demographic characteristics are broadly consistent with those of the Greater Manchester population (UK Population Data, 2023). In terms of ethnicity, the majority of respondents identify as white/British/European (62.80% in our sample compared with 66.7% in Greater Manchester), followed by Asian/Chinese/Vietnamese/Indian/Pakistani/Korean (21.5% in our sample compared to 17.1% in Greater Manchester) and Black (7.4% in our sample compared to 8.6% in Greater Manchester). A total of 122 citizens participated in the questionnaire and the data was analysed using descriptive statistics.

The first stage of data collection provided insights that informed the design of the main method employed in the research – a series of small-scale citizen workshops. Workshops are useful in identifying and exploring incompletely-defined challenges and experiences in research areas involving emerging technology, where research participants may find it difficult to articulate views about the topic (Ørngreen and Levinsen, 2017). In the workshops, a range of smart city applications, from apps to smart bins, were introduced and discussed in an interactive presentation that invited group discussion, peer feedback and creative practical tasks including drawing. The workshops aimed primarily to assess participants' understandings of data privacy, and identify privacy concerns and practices in their everyday lives.

Five two-hour workshops were conducted – four in-person, one online via Microsoft Teams – with a total of 30 citizens participating. Workshop participants were recruited with help from various local community groups so they formed a diverse collection in terms of their age, gender, education level and ethnicity (see Table 1). All workshops were audio recorded, ensuring all data was captured accurately, transcribed by research assistants and analysed using thematic analysis. the University of Salford Ethical Approval Committee (approval number 5266) and Manchester Metropolitan University Arts and Humanities Research Ethics and Governance Committee (approval number 11258). The questionnaire was delivered online and completed anonymously. It contained an information sheet about the project presented to respondents at the start of the survey. Participant information sheets and consent forms were presented to interviewees and workshop participants prior to securing their consent to take part in the research. All data gathered was treated anonymously.

Case study evidence and discussion

In this section, we use empirical data to examine and compare perspectives on data privacy in Manchester articulated by citizens and digital policy makers.

Context: Awareness and understanding of smart cities. Despite the extensive press coverage around Manchester's CityVerve project, in the empirical work conducted for this article, only 34.4% of questionnaire respondents had heard of the term 'smart cities'. In attempting to explain what a smart city is, some simply stated that the term had 'no meaning' or that they were 'not clear about it'. One respondent admitted, 'heard of it but don't understand what it means'. Others had very vague ideas of what a smart city describes and provided incomplete answers including, 'Working together towards regeneration' and 'interaction between cities'. However, most explanations included references to 'IT' or 'technology' and 'data'. This was corroborated by the workshop data, where, at the start of the sessions, not a single participant was able to confirm with any confidence that they understood what the term 'smart city' means.

The fact that citizens struggled to explain what a smart city is points to an identified obstacle to the global trend towards smart cities – the name itself, which is a vague term (Mathis and Kanik, 2021). Although perhaps tempting to use for city branding purposes (Interview Participant A explained how Manchester was branded 'The Information City', then 'The Digital City' and then 'The Smart City' in an attempt to capture the city's digital innovation history and credentials), the term 'smart city' is not particularly descriptive or meaningful to people.

Perhaps if CityVerve had produced results that Manchester citizens could see, the term 'smart city' might have been more meaningful to them. However, interview data shows that CityVerve exemplified the ongoing challenges of rolling out smart city initiatives in a citizen-participative way. It was argued that 'CityVerve was simply a project… it didn't really work at the end of the day' (Interview Participant A). Interview Participant A explained that some initiatives under CityVerve continued for the full two years of the project even though they 'weren't working', whereas some other, more promising initiatives that started later because they took longer to set up 'came to an abrupt end when the funding ended' and no follow-on funding was made available. Interview Participant A's assessment of CityVerve was echoed by Interview Participant B, who commented: 'We were essentially given two years and £10 million and a consortium of 30 partners to deliver a kind of smart IoT demonstrator ...Obviously, two years is not a lot of time…'. So although some technologies, including smart bus stops and smart bins, were trialled, they were never mainstreamed, either because they were not considered priorities in the same way as unemployment and poverty, or because they would cost too much. Interview Participant A explained: 'Manchester…, doesn't own its lamp posts. They're outsourced under historic PFI [public finance initiative] agreement to Amey [a commercial entity]. So anyone who wanted to do smart lighting would have to pay Amey £200 per lamp post for doing what in other areas they're able to do for free'.

Attitudes to data privacy. After watching a video explaining what a smart city is and discussing specific smart city applications and examples of smart technologies in Manchester (from apps to smart bins and smart metres), many of the workshop participants expressed indications of mistrust around data collection practices and privacy. Workshop Participant 3B identified privacy as 'the biggest concern' in smart cities, adding, 'What data are they getting and where's our data going?' Given a definition of data privacy to reflect on, workshop participants noted that citizens in a smart city no longer have the 'power to control' who has access to their data (Workshop Participant 5C). Workshop Participant 4A noted that 'We have the definition that you showed us before, but we have to think about privacy in the year that we are in…and I think the privacy that we mean doesn't exist no more'.

The local authority is also concerned about citizen privacy, although this was not the case when CityVerve was being rolled out. According to Interview Participant A, it was only during the development of the 2022 Digital Strategy, when the first draft was criticised by academics and

citizen groups, that the local authority started to take citizen privacy seriously. 'If you asked… the new leader of [the] council, what are the key challenges? [They] would say, privacy and social responsibility, ethical issues. That's one of the things. And that wasn't the case at the beginning. That was seen as a kind of minor issue'. Interview Participant C confirmed that privacy is now an important feature of the council's digital strategy, noting that perhaps in the past technological development and roll out per se predominated digital initiatives. And Interview Participant B agreed: '…we don't think of privacy as an add on…it's built in, you know…it's about reassuring your senior managers that we're not going to be on the front page of the *Daily Mail*…and the second thing is that we have actually got legal responsibilities as an information controller'.

Awareness of and trust in data practices in a smart city. Under the UK Data Protection Act 2018, citizens have the right to object to how their data is processed, but this right is impossible to exercise if they do not know who the local authority shares their data with and how this data is used. In fact, only 27.6% of the questionnaire respondents attempted to answer the question 'Name one orga-nisation that the local authority shares your personal data with'. Following a conversation among workshop participants, a consensus of mistrust was in evidence in the view that people do not know who has access to the data they share with their local authorities, prompting workshop participant 3C to ask: '…how do you trust someone you don't know?' After looking at a webpage with some terms and conditions for using open wifi in Manchester, none of the workshop participants indicated increased confidence or trust in data practices in their city because they found the information vague. Workshop Participant 5B suggested: 'If it's going to generate money for them, they'll be vague so that you can't go back on them, I suppose'. Workshop Participant 1A noted: 'You look at the list of their partners and they have something like 15, so every single person has this data? So it's really, where does it end, where does the buck stop?'

Only 23.8% of the questionnaire respondents were confident in their ability to manage who has access to their personal data, while only 13.1% knew what rights they have over how their data is used by their local authority and 50% were concerned about how the local authority uses their data. Concerns about how data is collected and used in a smart city were also expressed by many workshop participants. One noted that 'information passes so quickly it's hard to, once it's out there, to kind of say, well, where's it gone? It's just passed on fast so then, yes, you have the right to know, but you can't keep up with it' (Workshop Participant 5C). Another contended that 'They need to be more honest with what they are offering and where the information is going because I haven't got a clue, I don't even have a smartphone, so I'll probably be the least savvy of all of you in that sense' (Workshop Participant 1C). Workshop Participant 1A argued that many people 'have no idea what's going on' in smart cities and that this works to the advantage of smart city architects: 'And I'm not even talking about what's happening with my data. Where are the smart sensors being placed? What sensors do you have? What are your capabilities? And I wonder if this lack of knowledge on the citizens' part is intentional by the powers that be. Because if you have an informed public on how to protect its data, then their sensors etc… become less efficient. So are they worried about an informed public?' Mistrust was a common theme in the workshops and stemmed largely from 1) negative personal experiences of digitalisation in general or 2) sceptical opinions of central government and tech companies. Some participants mentioned being 'lied to' by the government during the Covid pandemic and one used the example of Cambridge Analytica to claim that data is not safe with profit-driven tech companies. Others described incidents where they or a family member lost money as a result of online fraud. The fact that smart cities operate through public-private partnerships and are seen to use a 'top down', 'technocratic approach' added an extra layer of mistrust, as Workshop

Participant 1A articulated: 'I read another quote the other day saying that hypothetically if George Orwell's 1984 came alive today it would be a public-private partnership'.

Yet, the interview data indicates efforts by the local authority and its consultants to inform the public on smart city initiatives, which were hampered by limited resources. Interview Participant A describes citizen engagement efforts via Zoom for the Digital Strategy in the time of Covid-19 as 'the art of the possible'. They explain: '…we went to Future Everything, Open Data Manchester, the CoOp Foundation, the AI Foundry, Citizens Advice Bureau and so on and said, you know, well, you're in touch with real people who are suffering through the pandemic. What can you feed into us? Because that's you know, that's all we have the capacity to do. So on one hand, does that stand up to an objective analysis of citizen participation, engagement? Probably not. Was citizen engagement thought about as we developed the digital strategy? Absolutely yes, all the time'. Interview Participant B admitted that 'there has been quite a bit of lip service to community engagement and community consultations', and Interview Participant A agreed that this was the case in the past, but argued that the local authority has learnt some valuable lessons in the process of developing its digital strategy and now has a much better understanding of, and commitment to, citizen data rights. Interview Participant C noted that the council has worked with Open Data Manchester, a non-profit organisation that aims to promote responsible data practices, to gain a better understanding of data handling issues. Participant C also argued that working successfully with communities, possessing a 'people first' outlook and being able to communicate effectively with members of diverse communities are features of effective digital leadership, and provided examples of the work that the newly established Greater Manchester Digital Inclusion Taskforce has done recently, including a series of 'roadshow' events in public spaces like shopping centres and museums where people were asked their views about digital technologies and services.

Mistrust, data privacy and local authority governance. Although interview Participant A argued that 'local authorities are still trusted' and that 'we put a lot of effort in to gain that trust', only 32% of the questionnaire respondents indicated that they trusted the local authority with their personal data. In the workshops, people expressed distrust about the local authority's private sector partners. Workshop Participant 3D argued that '…the thing with local authorities is… you have a trust in that phrase. It feels like it's a name that you should trust. But if they're being funded and they're sharing their stuff with third parties in the private sector…' Workshop Participant 1A commented that 'the city council is not a tech company, they don't know how to put smart sensors in their train stations, they can partner with someone to do that. How is that lucrative to their partners? Well, the people's data, they can sell it'. Asked directly whether they trusted private companies less than their local authority, Workshop Participant 3D said: 'I don't trust anyone. But I trust someone trying to make money from me less than someone who is just maybe not as good at their job'. This finding is consistent with Kennedy et al. (2022) who found that people are concerned about the involvement of commercial companies in public sector data uses. It also echoes sentiments that have stalled smart city initiatives around the world, including the City of Toronto in Canada (Kitchin, 2019; Nisenbaum, 2019).

There was evidence in the workshops of a wider mistrust of technology, where concern was expressed about 'things breaking down', 'data corruption', 'hacking' and excessive 'reliance on the system'. One participant observed that 'The Internet… went down for four of the big hospitals recently… It was taking weeks to get operations and to get counselling, people couldn't go in' (Workshop Participant 2A). Asked whether data security was a concern, most of the workshop participants indicated agreement, with Workshop Participant 2B noting 'Yes, because there's always somebody smarter than you'. This finding is consistent with a documented backlash against

technology, or techlash, which reflects rising societal concerns about the rapid pace of technological development and the security and privacy risks this may entail (Guarini, 2021). According to a recent survey from Edelman (2021) trust in the technology sector has fallen globally by 9% (from 77% to 68%) between 2012 and 2021 – a finding reflected in the questionnaire data, where search engines (2.5%), social media companies (4.1%) and telecom companies (6.6%) are the three least trusted organisations.

Yet, concerns about technology companies were also evident in the interviews with city planners. Interview Participant A claimed that, at the time of CityVerve, 'there was no one from the tech companies talking about privacy, apart from the process driven thing, you know, we must tick all the boxes'. Interview Participant B gave an example from CityVerve of how they had to explain to a private sector partner why they could not install surveillance cameras on a main road in Manchester, stating that although the local authority had 'every faith' in their partners in 'sorting out the tech and creating secure systems', they were less confident in their consideration of 'the ethical dimension'.

The paradox of mistrust and participation in smart city initiatives.   Even though privacy is now clearly an important consideration for the local authority, Interview Participant A was hopeful that citizens would not object to smart initiatives based on privacy concerns, if they were going to improve security. They offered an example from a community forum about CCTV 30 years ago, where citizens said they would want this technology on every street corner, if it was going to make their streets safer. Additionally, although privacy is very important, it was argued that people have more pragmatic concerns, including 'work, jobs, income, poverty, health…' This is corroborated by the questionnaire data, where 40.2% of respondents agreed or strongly agreed with the statement 'I am happy to give up some of my privacy if it improves my quality of life in a city'. They indicated a willingness to concede personal data in return for health, safety and financial benefits.

Despite the afore-evidenced mistrust, there were also indications in the workshops that participants would be happy to give up some of their privacy if they could see direct results from it in the shape of increased convenience, savings in energy bills, sustainability and better functioning cities. Workshjop Participant 4D noted that: '…if it's kind of clear how they use our information, if they're using it to make things better, then for me… I don't really mind about tracking me or like using my personal data'. However, Workshop Participant 2D argued that privacy 'continues to be eroded in the name of security', where new technology is pushed through as a short-term measure following an emergency (e.g. Covid, terrorism) and eventually becomes normalised. Interestingly, citizens distinguished between smart city applications, describing some as more useful, and therefore more worthy of their data, than others. Smart motorways, for example, were seen by many as unnecessary: 'I just don't see what has been done that is different. Still crowded. Just as crowded as it was beforehand' (Workshop Participant 1F). Smart metres had a more mixed response from participants, with some questioning their usefulness and others saying they were happy to allow their energy providers to track their daily routines for the sake of convenience and reduced energy bills. Our findings are consistent with evidence from the literature that, given the opportunity and incentives, citizens are willing to participate in co-production of public services with governments in the delivery of 'smart' programmes (Coutinho et al., 2019). However, only 6.7% of the questionnaire respondents would be willing to give up personal data for 'personalised adverts and offers', supporting Van Zoonen's (2016) hypothesis that people are less likely to raise privacy concerns if the data collected is used for the purpose of enhancing city services.

When asked what their local authority could do to get people on board with their smart city vision, many workshop participants suggested raising awareness about how a smart city works and what the benefits are to residents. One noted, 'I think if they think it's such a big advantage to the

citizens living in Manchester then they should be putting out more things in the news to let people know what's going on and why it's advantageous to them' (Workshop Participant 1D). Another argued that: 'I'm more inclined to give my data 'cause I'm seeing the benefit of what it could be. If you're not seeing what is becoming of it, then you're going to be more reluctant …' (Workshop Participant 4B).

Participants also wanted 'to be consulted and also involved' in smart city projects (Workshop Participant 4C), more transparency about how data is collected and used, and some control over what personal data is stored and for how long, one noting the need 'to be honest with where the data is going and what they're doing with it?' (Workshop Participant 2B). Very importantly, citizens were proactive in making suggestions, such as 'I want access to raw data to be restricted completely… and then maybe beyond that like a way to maybe opt out maybe for ordinary people. People could also look at whatever data specifically pertains to them, delete it if they don't….' (Workshop Participant 2D) and 'I would say like an open platform where you can log in with your details and you can actually manage what has been collected and you can see how your data is actually being used. And you can either decide that it's okay with you or…I give you my data but if I don't want you to have my data no more, I can withdraw it without any consequences' (Workshop Participant 4A).

Conclusion

The evidence of citizen privacy experiences and concerns from the case highlighted in this article contrasts in significant part with those of policy makers charged with delivering effective smart digital technology-underpinned initiatives. The article, through case study analysis, adds to the existing critical work of scholars such as Cardullo and Kitchen (2019) and Breurer and Pierson (2021) by highlighting the detailed concerns of people in smart cities regarding data privacy, in the process illustrating mistrust manifesting as scepticism, frustration and vigilance, yet also the willingness to engage with policy makers in order to realise the benefits of smart city developments. It extends the literature on smart cities by presenting the, on the surface counterintuitive, argument that the existence of mistrust – in abundant evidence in this article – has the potential to create the conditions for enhanced citizen participation in smart city initiatives through addressing privacy concerns.

Even in cities like Manchester with a long history of attempts to harness digital technologies and services for public benefit, our evidence underlines the core challenge of developing trust among people through a deeper process of engagement. Although evidence suggests that the local authority values citizen data privacy, it currently lacks the resources and expertise to reach out extensively and meaningfully to citizens to secure deeper participation, and is largely dependent on private partners that may not share its values and are clearly *distrusted* by its citizens. Smart city initiatives can only succeed if citizens develop more trust in those in charge of their data because they know their human rights will be safeguarded, and they can make an informed digital choice to engage with these initiatives. In line with the idea of *mistrust* as a flexible concept with critical and participatory democratic credentials, evidence also suggests a willingness among citizens to adopt smart city technologies if their broad practical utility and value and integrity can be established. This is matched in our evidence by a stated desire among policy makers to address citizen data privacy concerns and offers a way forward.

Further empirical work is needed to explore how citizens and policy makers can close the smart city trust and participation gap which exists between them. Here, it is important to understand that there are sections of the population who are unwilling and/or unable to engage with smart civic

services. Evidence in this article suggests that there is a significant need for more effective and meaningful ways of consulting with – and understanding the perspectives of – the people who are the intended recipients of new digital technology-underpinned 'smart' services. This article has found evidence of 'tokenism' and 'consultation and placation' but also the potential to move towards more participative strategies delivering 'citizen power' and even 'co-creation' (Cardullo and Kitchen, 2019). This can be achieved through harnessing the vigilant mistrust in evidence among citizens through the creation of a digital cities and privacy working group at metropolitan/ council level, comprised in equal measure of citizens and policy makers, to develop a plan for citizen engagement to unfold over the short to medium term. Methodological evidence from this article points to the value of running several series of face-to-face data privacy workshops between local authorities and citizens to gather large scale in-depth evidence of the concerns of people regarding the use of smart technologies, in order for the local authority to develop detailed understandings of the lived privacy concerns of citizens.

From this, a City Digital Rights and Privacy Charter approach could be developed. In complement, a living (in other words open and developing) roster of citizen privacy issues in digital applications design could be co-created and used in procurement processes with technology systems designers. Citizen privacy protection could then become an essential indicator to demonstrate in procurement processes and be made a condition of award in contracts for smart digital applications and services. Thereafter, the requirement to engage with citizens and civil society organisations at key junctures of the smart applications and service design process could be established. Actions such as this could realise and make residual Lenard's (2008: 313) idea of vigilance 'motivated by an attitude of mistrust whilst *simultaneously* demanding the existence of widespread trust relations' (emphasis in original). In so doing, the gap between policy maker and citizen understandings and expectations of data privacy can be narrowed and the public value of smart technologies in urban environments further realised.

ORCID iD

Seamus Simpson   https://orcid.org/0000-0003-1814-4224

References

Albino V, Berardi U, and Dangelico RM (2015) Smart cities: definitions, dimensions, performance, and initiatives. *Journal of Urban Technology* 22(1): 3–21. DOI: 10.1080/10630732.2014.942092.

Bakici T, Almirall E, and Wareham J (2012) A smart city initiative: the case of barcelona. *Journal of the Knowledge Economy* 4(1): 135–148.

Beldad A, van der Geest T, de Jong M, et al. (2011) A cue or two and I'll trust you: determinants of trust in government organizations in terms of their processing and usage of citizens' personal information disclosed online. *Government Information Quarterly* 29: 41–49.

Bogard W (1996) *The Simulation of Surveillance: Hypercontrol in Telematic Societies*. Cambridge: Cambridge University Press.

Bräunlich K, Dienlin T, Eichenhofer J, et al. (2021) Linking loose ends: an interdisciplinary privacy and communication model. *New Media & Society* 23(6): 1443–1464.

Breuer J and Pierson J (2021) The right to the city and data protection for developing citizen-centric digital cities. *Information, Communication & Society* 24(6): 797–812. DOI: 10.1080/1369118X.2021.1909095.

Caird S (2018) City approaches to smart city evaluation and reporting: case studies in the United Kingdom case studies in the United Kingdom. *Urban Research & Practice* 11(2): 159–179. DOI: 10.1080/17535069. 2017.1317828.

Calzada I (2021) The right to have digital rights in smart cities. *Sustainability* 13(20): 11438. DOI: 10.3390/su132011438.

Cardullo P and Kitchin R (2019) Being a 'citizen' in the smart city: up and down the scaffold of smart citizen participation in Dublin, Ireland. *Geojournal* 84: 1–13.

Carter D (2019) *Manchester's Urban Regeneration – from the 'original, Modern' City through Creative and Digital Strategies to a Smart Future City*. Oxford: University of Manchester. unpublished paper.

Citrin J and Stoker L (2018) Political trust in a cynical age. *Annual Review of Political Science* 21: 49–70.

Coutinho MM, Vasconcellos Sobrinho M, Oliveira SACM, et al. (2019) Coprodução Sociedade Civil - Governo na Constituição de Cidades Inteligentes no Estado do Pará. *Revista de Administração Contemporânea* 23(5): 636–653.

Cowley R and Caprotti F (2019) Smart city as anti-planning in the UK. *Environment and Planning D: Society and Space* 37(3): 428–448.

De Zwart M, Humphreys S, and Van Dissel B (2014) Surveillance, big data and democracy: lessons for Australia from the US and UK. *UNSW Law Journal* 37(2): 713–747.

Eckhoff D and Wagner I (2017) Privacy in the smart city—applications, technologies, challenges, and solutions. *IEEE Communications Surveys & Tutorials* 20(1): 489–516.

Edelman (2021) *Edelman Trust Barometer 2021*. [Online]. https://www.edelman.com/sites/g/files/aatuss191/files/2021-03/2021_Edelman_Trust_Barometer.pdf.

Eger JM (2009) Smart growth, smart cities, and the crisis at the pump a worldwide phenomenon. *I-Ways* 32: 47–53.1.

Finch K and Tene O (2013) Welcome to the metropticon: protecting privacy in a hyperconnected town. *Fordham Urb LJ* 41: 1581. https://ir.lawnet.fordham.edu/ulj/vol41/iss5/4.

Flyvbjerg B (2006) Five misunderstandings about case-study research. *Qualitative Inquiry* 12(2): 219–245.

Foucault M (1977) *Discipline and Punish: The Birth of the Prison*. London: Penguin Books.

Global Data (2022) *Smart Cities Market Size, Share, Trends, Analysis and Forecasts By Region, Application (Smart Transportation (Intelligent Transportation, Parking Management, Smart Ticketing), Smart Infrastructure (City Surveillance, Smart Lighting, Command & Control Systems), Smart Grid, Smart Building, Smart City Platforms), and Segment Forecast to 2026*. https://www.globaldata.com/store/report/smart-cities-marketanalysis/?_gl=1*nyq4lk*_ga*MjA5NTQyNTMwOS4xNjkxNjYyMjEy*_ga_JYSQW15TQG*MTY5MTY2MjIxMS4xLjAuMTY5MTY2MjIxMS42MC4wLjA.

Gov.uk (2015) *Manchester Wins £10m Prize to Become World Leader in 'Smart City' Technology*. https://www.gov.uk/government/news/manchester-wins-10m-prize-to-become-world-leader-in-smart-city-technology.

Greater Manchester Combined Authority (2020) *Greater Manchester Digital Blueprint (2020-23)*. https://www.greatermanchester-ca.gov.uk/media/6275/gmca_blueprint_jul-22.pdf.

Guan L (2012) Smart steps to A battery city. *Government News* 32(2): 24–27.

Guarini K (2021) *A rising Distrust of Science and technology*. Mother of Invention. https://mother-of-invention.net/2021/07/19/a-rising-distrust-of-science-and-technology/.

Gubbi J, Buyya R, Marusic S, et al. (2013) Internet of Things (IoT): a vision, architectural elements, and future directions. *Future Generation Computer Systems* 29(7): 1645–1660. DOI: 10.1016/j.future.2013.01.010.

Hilden J (2019) *The Politics of Datafication – the Influence of Lobbyists on the EU's Data Protection Reform and its Consequences for the Legitimacy of the General Data Protection Regulation*. Helsinki: Publications of the Faculty of Social Sciences, University of Helsinki.

Hollands RG (2008) Will the real smart city please stand up? Intelligent, progressive or entrepreneurial? *City* 12(3): 303–320. DOI: 10.1080/13604810802479126.

Jennings W, Stoker G, Valgarðsson V, et al. (2021) How trust, mistrust and distrust shape the governance of the COVID-19 crisis. *Journal of European Public Policy* 28(8): 1174–1196. DOI: 10.1080/13501763.2021. 1942151.

Kennedy H, Oman S, Taylor M, et al. (2020) *Public Understanding and Perception of Data Practices: A Review of Exsiting Research*. https://livingwithdata.org/project/wp-content/uploads/2020/05/living-with-data-2020-review-of-existing-research.pdf.

Kennedy H, Oman S, Ditchfield H, et al. (2022) *Data Matters are Human Matters: final Living With Data Report on Public Perceptions of Public Sector Data Uses*. https://livingwithdata.org/project/wp-content/uploads/2022/10/LivingWithData-end-of-project-report-24Oct2022.pdf.

Kitchin R (2014) The real-time city? Big data and smart urbanism. *Geojournal* 79(1): 1–14. DOI: 10.1007/s10708-013-9516-8.

Kitchin R (2019) *The Ethics of Smart Cities*. https://www.rte.ie/brainstorm/2019/0425/1045602-the-ethics-of-smart-cities/.

Knijnenburg BP, Page X, Wisniewski P, et al. (eds) (2022) *Modern Socio-Technical Perspectives on Privacy*. https://ebookcentral.proquest.com/lib/mmu/detail.action?docID=6885922 (Accessed 6 February 2024).

Lara AP, Da Costa EM, Furlani TZ, et al. (2016) Smartness that matters: towards a comprehensive and human-centred characterisation of smart cities. *Journal of Open Innovation: Technology, Market and Complexity* 2(8): 1–13. DOI: 10.1186/s40852-016-0034-z.

Lenard PT (2008) Trust your compatriots, but count your change: the roles of trust, mistrust and distrust in democracy. *Political Studies* 56: 312–332.

Manchester City Council (2020) *Manchester Digital Strategy*. https://www.manchester.gov.uk/info/500002/council_policies_and_strategies/8356/manchester_digital_strategy_2021_–_2026.

Martin CJ, Evans J, and Karvonen A (2018) Smart and sustainable? Five tensions in the visions and practices of the smart-sustainable city in Europe and North America. *Technological Forecasting and Social Change* 133: 269–278. DOI: 10.1016/j.techfore.2018.01.005.

Marwick A and Hargittai E (2019) Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. *Information, Communication & Society* 22(12): 1697–1713. DOI: 10.1080/1369118X.2018.1450432.

Mathis S and Kanik A (2021) *Why you'll be hearing a lot less about 'Smart Cities'*. City Monitor. https://citymonitor.ai/government/why-youll-be-hearing-a-lot-less-about-smart-cities.

Myeong S, Park J, and Lee M (2022) Research models and methodologies on the smart city: a systematic literature review. *Sustainability* 14(14): 1687. DOI: 10.3390/su14031687.

Nisenbaum A (2019) *What's Holding Smart Cities Back? 18th March*. Scientific American Blog. https://blogs.scientificamerican.com/observations/whats-holding-smart-cities-back/.

Nissenbaum H (2004) Privacy as contextual integrity. No1 symposium, technology, values and the justice system. *Washington Law Review* 79: 119–158. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10.

OECD (2020) *Cities Policy Responses*. https://read.oecd-ilibrary.org/view/?ref=126_126769-yen45847kf&title=Coronavirus-COVID-19-Cities-Policy-Responses.

Ørngreen R and Levinsen K (2017) Workshops as a research methodology. *Electronic Journal of e-Learning* 15(1): 70–81.

Pali B and Schuilenburg M (2020) Fear and fantasy in the smart city. *Critical Criminology* 28(4): 775–788.

Rousseau DM, Sitkin SB, Burt RS, et al. (1998) Not so different after all: a cross-discipline view of trust cross-discipline view of trust. *Academy of Management Review* 23(3): 393–404.

Sadowski J and Pasquale FA (2015) The spectrum of control: a social theory of the smart city. *First Monday* 20(7). DOI: 10.5210/fm.v20i7.5903.

Sharifi A, Allam Z, Feizizadeh B, et al. (2021) Three decades of research on smart cities: mapping knowledge structure and trends. *Sustainability* 13(13): 7140. DOI: 10.3390/su13137140.

Shelton T and Lodato T (2019) Actually existing smart citizens: expertise and (non) participation in the making of the smart city. *City* 23(1): 35–52. DOI: 10.1080/13604813.2019.1575115.

Thomas V, Wang D, Mullagh L, et al. (2016) 'Where's wally? In search of citizen perspectives on the smart city'. *Sustainability* 8(3): 207. DOI: 10.3390/su8030207.

Trein P and Varone F (2023) Citizens' agreement to share personal data for public policies: trust and issue importance. *Journal of European Public Policy* 1–26. DOI: 10.1080/13501763.2023.2205434.

UK Population Data (2023) *Manchester Population 2023*. https://populationdata.org.uk/manchester-population/.

Utz S and Krämer NC (2009) The privacy paradox on social network sites revisited: the role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 3(2). https://cyberpsychology.eu/article/view/4223.

Van Zoonen L (2016) Privacy concerns in smart cities. *Government Information Quarterly* 33(33): 472–480.

Westin A (1967) *Privacy and Freedom*. New York: Atheneum Press.

Yin RK (2012) *Applications of Case Study Research*. 3rd edition. Thousand Oaks, CA: Sage Publications.

Zhang K, Ni J, Yang K, et al. (2017) *Security and Privacy in Smart City Applications: Challenges and Solutions*. Piscataway, NJ: IEEE Communications Magazine. https://ieeexplore.ieee.org/document/7823349.

Ziosi M, Hewitt B, Juneja P, et al. (2022) Smart cities: mapping their ethical implications. *SSRN Electronic Journal*. Amsterdam, The Netherlands: Elsevier. DOI: 10.2139/ssrn.4001761.