# The Social Construction of Personal Data Protection in Smart Cities

Jonas Breuer
*imec-SMIT,*
*Vrije Universiteit Brussel*
Brussels, Belgium
Jonas.Breuer@vub.be

Ine Van Zeeland
*imec-SMIT,*
*Vrije Universiteit Brussel*
Brussels, Belgium
Ine.Van.Zeeland@vub.be

Jo Pierson
*imec-SMIT,*
*Vrije Universiteit Brussel*
Brussels, Belgium
Jo.Pierson@vub.be

Rob Heyman
*imec-SMIT,*
*Vrije Universiteit Brussel*
Brussels, Belgium
Rob.Heyman@vub.be

***Abstract*— Cities are striving to become 'smart'. What exactly a smart city signifies is debatable, but the designation most often refers to an intensification of ICT use and data use by local authorities, and seeking closer collaboration with other stakeholders. Whereas the concept of the smart city is not clearly delineated, the same can be said for the requirements for personal data protection under the GDPR. In this paper, we apply a social constructivist approach to the development of personal data protection in smart city initiatives to argue that personal data protection in smart cities is in a stage of 'interpretative flexibility', implying that different groups put forward different meanings to these concepts. Based on a quasi-empirical scenario analysis, we assess interpretations, opportunities and challenges related to the most influential actors and factors. To conclude, we formulate a number of specific recommendations for privacy-friendly implementation of smart city initiatives.**

***Keywords—smart city, personal data protection, SCOT, scenarios, participation, privacy***

## I. Introduction

Cities are expanding their efforts to become 'more digitalised,' 'more intelligent,' and 'smarter' [1]. The concept of the 'smart city' is not clearly delineated: conceptualizations encompass elements such as improved city management and organisation, technology use, governance, policy, people and communities, economy, infrastructure, and natural environment [2]. In general, core components of smart city initiatives include an increased use of information and communication technologies (ICT); increased usage, sharing, and re-use of data; and increased collaboration between various stakeholders [3]. What a smart city comes to be therefore depends on different actors and factors, their interests and interpretations, as well as interdependencies between them. This is partly reflected in the Quadruple Helix approach [4], widely adopted by European Union institutions, which regards innovation as the outcome of an interactive process between different spheres of actors; industry, government, academia, and civil society.

It has been pointed out that corporate interests often dominate in the shaping of smart city initiatives [5]–[8], while citizen voices are less present in the decision-making process. The European Union's General Data Protection Regulation (GDPR)[1] could become an instrument in strengthening the influence of citizens, as it entails increased accountability and more transparency in the processing of personal data. One could argue that, to develop smart city initiatives that meet the value of accountability - core to the GDPR, but also core to public administration overall - it is essential to take the needs of citizens into account. However, the practical implementation of GDPR requirements also needs to contend with other actors and factors: existing contracts with vendors and ICTs already in use, conflicting legislation, a limited set of practical options, contextual restrictions, legacy IT systems, and so on. This creates a contested space of competing interests, where different stakeholders try to impose their interpretations and definitions. Here, mutual-shapings between smart city technologies and data protection practices can be observed.

In this paper, we investigate the development of personal data protection in smart city initiatives from a social constructivist perspective. This approach presents a starting point for long-term analyses of the social construction of personal data protection in smart cities.

We argue that the handling and protection of personal data in smart city initiatives should not just be studied as a consequence of legal intervention, but as a socio-technological process in which different actors and factors play roles in shaping outcomes. The leading question for the analysis is: What are different meanings and interpretations that relevant groups attach to data protection related requirements, and how do they influence the smart city personal data protection regime? To provide practical recommendations to smart city initiatives and public administrators, we follow a scenario-based approach, which is defined in chapter three, after the theoretical foundations are clarified in chapter two. Chapter four provides three different scenarios, and chapter five discusses main aspects before a set of recommendations are provided in chapter six. A short conclusion rounds-up the analysis.

## II. Theoretical Framework

To assess the socio-technological process in which personal data protection is being put into practice in the smart city, we take a social constructivist perspective, as part of the broader field of Science and Technology Studies (STS) [9]. STS takes as its "central concern the ways that materiality, practice, and politics are necessarily entangled" [10, p. 9]. Technology is analysed as in motion, a process shaped by different actors and factors. The process becomes stabilised

[1] Regulation (EU) 2016/679 eur-lex.europa.eu/CELEX:32016R0679

when "once-contested technologies seem to settle into some comfortable frame of understanding" [10, p. 14]. An analysis must therefore account for dynamic (not pre-set or linear) links and interdependencies among artefacts, practices and social arrangements [11, p. 3]. This idea has recently been taken up in the fields of infrastructure studies and platform studies, two theoretical approaches that further improve the understanding of new artefacts and their interdependencies with practices and social arrangements [12].

The social constructivist perspective adopted for this article is rooted in the 'social construction of technology' (SCOT) framework suggested by Pinch and Bijker [13]. They have shown that different stakeholders present different articulations of similar technologies, and that the technology that eventually dominates (i.e. 'stabilises') is most often chosen for non-technical aspects: eventual success of a particular technology a result of social agreements and convincing argumentation rather than technological benchmarking. The first stage in Pinch & Bijker's account of the development of technologies is one of 'interpretative flexibility', in which different social groups have radically different interpretations of a technology and different solutions compete for dominance. In the second stage, 'closure' mechanisms (e.g. redefinition of a problem or a 'knockdown argument') lead to agreement over and stabilization of a technology. In the final stage, those closure mechanisms are related to the wider social-cultural milieu.

The implementation of GDPR requirements in the context of the smart city is currently in a stage of interpretative flexibility; open, while different groups strategize to put forward their interpretations of the requirements. The strategies of these groups are aimed at convincing other stakeholders to adopt the solutions most beneficial to their agendas. The GDPR is interpreted and translated towards particular solutions (templates, procedures, information notices etc.) that shape personal data protection in smart city initiatives.

To analyse the 'interpretative flexibility' stage, relevant social groups are identified based on the question: For whom does personal data protection in smart cities have a similar meaning? **Smart city administrators** fulfil the requirement of the 'relevant social group' designation as users of smart city applications [13, p. 414]. They may not attach the exact same meanings to personal data protection in smart city initiatives at an individual level, but their interests and associated interpretations emerging from their positions in their administrative functions are likely to be similar. **Smart city technology vendors** can be identified as a 'relevant social group' in their role as solution providers. They are also likely to attach similar meanings to personal data protection in smart city initiatives, e.g. "fuel application development of city data".[2] In the interest of accountability with regard to new technologies with uncertain impacts, **citizens** must also be considered a 'relevant social group' [14]. A fourth relevant group, partly as a consequence of the Quadruple Helix approach advanced by the European Union, are **academic experts** in (personal data protection in) smart cities.

Taking the social constructivist perspective one step closer to an actor-network approach [15], we add **context** (i.e. smart city) and **smart city technologies** as relevant factors themselves, which cannot be overlooked in the articulation of personal data protection in smart cities. Here we can observe a mutual shaping process: interpretations of the GDPR are shaping smart city initiatives, and those initiatives are shaping personal data protection.

At this early stage of research, and due to the 'interpretative flexibility', we are mostly interested in the different meanings and interpretations that different groups attach to the requirements, as we believe 'closure' has not yet come about. This article is an initial attempt, a starting point in analysing the social construction of personal data protection in smart cities. Undoubtedly, subdivisions must be made - for instance, the meanings that smart city initiatives will have for different subgroups of citizens will depend on their level of involvement or digital literacy - but we leave those for more extensive analyses in future studies.

## III. Methodology

The application of data protection legislation in the city is a relatively new phenomenon and impacts cannot be easily predicted, due to the novelty of the situation. Nevertheless, practical GDPR interpretations are becoming more and more prevalent in technology implementation and change is becoming increasingly difficult to achieve, as technology becomes stabilised. Similarly, data protection practices will crystallise and become harder to oppose. Such 'stabilisation' can become a closure mechanism, but we are not in such advanced stages yet.

To account for the current stage of 'interpretative flexibility', we adopt the Quasi-Empirical Scenario Analysis (QuESA) [16], which presents scenarios as plausible storylines that represent an imagined but realistic world, with the potential to provide insights into an emergent, new context. We chose the scenario analysis as a technique of long-term strategic planning [17] to identify possible trends of plausible futures and to outline strategic choices, in order to be able to formulate specific recommendations for decision-makers. The following scenarios are quasi-empirical because they originate in real-life situations, but are extended with hypothetical or speculative elements. They stem from different Flemish smart city projects in which the research group imec-SMIT/VUB is involved as a major partner.[3] Each scenario is generalized in order to encompass a range of issues not all of which will arise in any particular real-life situation. The intention is not to substitute case studies but to test assumptions regarding personal data protection in the smart city.

Each scenario is followed by an overview of the perspectives of each of the four relevant groups of actors, as well as the influence of the context and technology. As these overviews merely serve to illustrate the type of analysis we propose, we present no more than the outlines of the analysis.

## IV. Scenarios

The following scenarios are based on real-life examples from Flemish smart city initiatives. After each scenario, we describe meanings of personal data protection and agency for the four relevant social groups in the context of that scenario, and the 'agency' of context and technology. The implications of the scenarios are then discussed in more depth in chapter V.

[2] CISCO, 'What is a smart city?', retrieved on 10 April 2019, www.cisco.com/what-is-a-smart-city.html

[3] More information on the initiatives and projects that provided main insights for the QuESA can be found in the acknowledgments.

### A. Scenario 1) Museum

*A municipal design museum wants to track visitors to understand how they interact with the exhibitions. The project requires a speedy public procurement process. As a result, the museum ends up having to choose between a number of tracking solutions, like inaccurate WIFI-sniffers, facial recognition image processing, and wearables that offer precise coordinates in 3D. Due to the invasive nature of the project, the legal department of the city is consulted. They advise to err on the side of caution: consent is safer and easier than public interest as legal basis for this type of processing of personal data. Cameras and WIFI scanners could track users that do not consent, so they are ruled out early. Wearables are the only option for consent as the legal basis, since these work through the affirmative action of choosing to wear one.*

***City administrators***, in this situation, are faced with a perceived need for visitor tracking and the GDPR requirement to determine a legal basis for this type of processing, combined with choosing a suitable technology. The issue for them is how to combine a data collection need with accountability requirements.

***Technology vendors*** see a situation in which their technology can meet a need for visitor tracking, and the issue is how to present their technology as the optimal solution for the city administrator, knowing that s/he will be considering technologies that stay within the boundaries set by the GDPR.

***Citizens*** see a situation in which their behavior will be tracked, and they may wonder whether that is necessary, but they may also accept the justification for the tracking (given sufficient explanation) and may expect benefits in the form of improved services, for example.

***Academia*:** Legal scholars see a situation with legal consequences, specifically a situation in which different legal grounds for processing are applicable. E.g. instead of consent, 'legitimate interest' can also be used as a legal basis for visitor tracking [18], [19], depending on the purpose of the tracking, and as long as the museum's interests are formally balanced against visitors' interests.

***Context*:** If the museum already contains tracking technology, such as security cameras, efficiency considerations will suggest repurposing. In that case, the default situation for visitors will be different from a situation with no tracking, influencing decisions on other types of tracking. The museum is also a clearly delimited physical space with an entrance that all visitors pass through (unlike a city centre), making it easy to discern data subjects and to inform them of tracking or to ask for their consent.

***Technology*:** Camera and WIFI-tracking technologies limit individual choice for data subjects, whereas wearable and smartphone-based technologies allow for more individual control. Whether data are registered, or automatically shared with other systems, or processed in the cloud, are all aspects ('affordances') that affect the potential for personal data protection.

### B. Scenario 2) Vendor Lock-in

*The administration of a medium-sized city has been working with a system, offered and controlled by a third-party supplier, to manage the data they are working with. This is common practice as it reduces costs, efforts and risks for the city, which cannot invest in developing their own systems. The system was purchased as a package that bundles different functions as well as the software with different data processing operations. This is now causing friction as the administration wants to ensure compliance with the GDPR. The old contracts do not include clear provisions for ownership of the data, access to it, or usage rights. The administration faces overwhelming practical difficulties when considering to change suppliers, systems, or contracts, or at least to determine with certainty who has access to and control over (personal) data, with which the administration works. The consequence is 'vendor lock-in' for the city administration.*

***City administrators***, in this situation, perceive GDPR requirements as pressure to change long-standing arrangements and relationships, but they lack actual means to enact those changes. The issue for them is the compliance with the legislation in the reality of their jobs, skills and (financial) capabilities.

***Technology vendors*** see a situation that presents risks to their business model. They might lose contracts standing perhaps for years, or at least are confronted with a changing supplier-customer relationship that used to be characterized by asymmetries in their favour. The issue is how to stay within the boundaries introduced by the GDPR, which might necessitate substantial changes to their business model.

***Citizens*** in this situation are not directly participating in the decision-making process. If they have any knowledge of it at all, they may perceive a situation where their elected representatives are powerless towards private companies, which may even be enabled to handle personal data according to their own rules.

***Academia:*** Legal scholars see a situation where the GDPR requirements can actually strengthen the negotiating position of public administrators. Several of its 'data subjects rights' requirements, for instance, entail that data processing by third parties must be transparent and that the processor can be held accountable [20]. The 'right to data portability' could prevent vendor lock-in caused by proprietary systems because it entails data formats that allow readability by other systems [21].

***Context:*** Public sector organisations have to follow strict procurement rules that need to be efficient but fair, transparent, and safeguarding the public interest. This context, although certainly necessary, often limits options and choices of public administrators.

***Technology:*** Data management software would be very difficult to develop, implement and maintain by most cities, making outsourcing the only feasible option. Furthermore, even when contractual arrangements withstand vendor lock-in, technological lock-in is likely to be considerable and might persist for such practical reasons as lack of time and budget, skill burden, knowledge deficiencies or frustration of colleagues.

### C. Scenario 3) Crowd measuring

*A city administration is approached by a technology vendor with an existing 'solution' to measure crowds in the city. The premise is that measuring crowds can enhance inner-city safety and security, improve experiences of local business, visitors and inhabitants by providing data about (bottlenecks to) crowd flows, and generate information to support policy decisions to improve liveability. The crowd*

*measurement would take place in public spaces with WIFI-tracking sensors. The technology has been tried and tested elsewhere; all the city needs to do is sign on (and pay). The city's administration considers the proposal and decides to review other options and vendors. Some use fixed cameras, some with face recognition, others by sensing body heat. There are even options that use drones. The administration is concerned because, according to their understanding of the GDPR, all of these options would fall under the regulation. In all cases, asking consent from inhabitants and visitors is out of the question: everyone moving in the public space would be measured.*

***City administrators*** are sensitive to the technology vendor's argumentation but recognize accountability risks. The issue for them is the proportionality of several varieties of means to collect personal data, not the proportionality of purposes. In assessing the proportionality of the means they are, however, also considering the legal basis.

***Technology vendors*** see an opportunity to present their solution to a city's needs. The issue to them is to balance personal data protection against other public interests, such as safety, smooth traffic, and crowd control, and make their solution stand out among competitors in this balance of interests.

***Citizens*** face a situation in which they will be tracked in public space, which may be to their benefit (e.g. security). The issue for them is how to attain those benefits while yielding the least of their anonymity in public. Another issue may be the extent to which data collected for public purposes will be used for revenue-generation purposes of private-sector actors.

**Academia:** Apart from debates over whether the legal basis of 'public interest' or 'legitimate interest' should be used in public-private partnerships, there is also the matter of whether the e-Privacy Directive[4] should apply instead of the GDPR when it comes to Internet of Things technology [22].

***Context:*** When public spaces are surveyed, there are few alternatives to data subjects but stay home or leave the city. Asking for consent is highly impractical in public space, which means other legal bases for processing personal data must be sought. Aside from that issue, there is a tension in public-private partnerships regarding control and access: all parties involved want to be data owners (economic framing), but no-one wants the responsibilities of data controllers (legal framing).

***Technology:*** Off-the-shelf technology leaves no room for situation-specific data protection adjustments to its functioning. For surveillance technology, privacy-invasive effects are a matter of degree.

## V. Discussion

The interests and understandings of different relevant social groups, as well as the factors of technology and context, constitute a complex network of links and interdependencies that shapes the implementation of personal data protection in the reality of smart cities. The arrow points both ways: personal data protection requirements can influence smart city initiatives as much as the initiatives influence personal data protection.

*Scenario 1)* on the museum illustrates that, in this stage of 'interpretative flexibility', concerns about compliance with the GDPR and its requirements can overshadow other important concerns (e.g. context specificities such as museum aesthetics, measurement accuracy, willingness to consent of data subjects, citizen involvement in decision-making). Early involvement of citizens could have prevented some of these concerns, but no room for that was afforded. The scenario accentuates that consent as a legal ground for processing defers data protection choices to the end of the process, or 'outsources' them, as visitors have to decide individually if they want to be tracked. A consequence can be biased data, because those that agree to tracking may differ from those that don't, and services would henceforth be adapted only to the preferences of the tracked. While legal scholars point out that consent may not be the most suitable legal basis (but rather legitimate interests or public interests, with consent only as a last resort when no other reasons can be found to process personal data), administrators prefer consent due to uncertainty about the criteria for other legal bases. This preference favours technologies that allow for consent over technologies that can only rely on other legal grounds for processing.

This relates to the notion that technology shapes data protection options. Sensors offer more or less control to data subjects, and sensors sometimes prescribe the legal ground for processing. While cameras offer little control (passers-by cannot choose not to be seen when in range), one can switch off WIFI on one's device when in range of a WIFI scanner. Both technologies are less suitable for consent or contractual obligations. Wearable devices (e.g. watches or lanyards), on the other hand, offer more control since wearing them or turning them on is optional, as is true for a smartphone app, which can ultimately be deleted. Accordingly, they are more suitable for consent or contracts.

*Scenario 2)* on vendor lock-in illustrates that asymmetric supplier-customer relationships and power imbalances can preclude negotiations on equal footing: local governments are not in the position to demand extensive changes to standard packages from technology behemoths that they are already using. Disentangling the organisation from the complications of legacy systems can be a major headache.

The GDPR can strengthen the negotiating position of government organisations by justifying demands for a certain level of transparency and technology specifications that also meet their own needs. This is due to its 'data subjects rights' requirements: the right to request access to data (or have them corrected or removed) for data subjects means that data processing by third parties must be transparent. The right to data portability entails that personal data must be readable by other systems, which incidentally also could prevent vendor lock-in caused by proprietary systems.

The concepts of pre-commercial or innovative procurement are also interesting in this context when it comes to new projects. Cities, especially smaller and medium-sized ones with less purchasing power, can benefit from banding together to prevent vendor lock-in for future contracts.

*Scenario 3)* on crowd measuring illustrates that technologies "off the shelf" can have disadvantages if the procurers do not understand consequences of a chosen

[4] Directive 2002/58/EC (eur-lex.europa.eu/celex:32002L0058)

partnership or technology. Public acceptance of a project can decrease if, for example, an international company is chosen that is perceived as harmful to privacy and might store sensitive data overseas.[5]

The scenario also implies that, while the GDPR lays down that the purpose determines which data are collected, different actors in the data-processing chain have different purposes; government authorities can rely on 'public interest' as a legal basis for processing citizen data while private companies can rely on 'legitimate interests' (avoiding consent in public space, not least because data subjects' only choice would be to leave the city). Multiple agreements may be needed to process data from a single project, which may reduce the required transparency and clarity of the arrangement. Related to this are tensions in public-private partnerships about control and access. All parties want to be data owners (economic framing), but no-one wants the responsibilities of data controllers (legal framing).

The GDPR is clear about data controllership[6]: those who determine the purposes and means of the processing of personal data are controllers. In practice, many parties in the data processing chain share some decision-making on purposes and means. (A consequence may be that city administrations and suppliers are forced to turn to 'joint controllership'.)

Lastly, smart city initiatives can take as their starting point a specific problem citizen perceive in their immediate environment rather than a popular technology. It is possible to reduce the technology push through systematic user research and, for example, living labs[7]. Citizen requirements can be identified and prioritised before other actors consider how their technologies can be implemented.

## VI. Recommendations

Based on the scenario analysis and the discussions above, the following practical recommendations can be made to smart city initiatives and public administrators:

1) **'Weaponize' the GDPR:** Data subject rights such as the right to access and the right to data portability can prevent 'vendor lock-in'. City representatives can use accountability requirements strategically to support their position in revising and renegotiating contracts, and pushing through more favourable conditions. Awareness of this strategic use of requirements must be raised among the various municipal departments that negotiate projects and contracts.

2) **Involve citizens early and regularly:** Rather than deferring choices for citizens until 'after the fact' by relying on consent, involve citizens early in the decision-making process, e.g. in balancing their interests and expectations versus proposed legitimate or public interests. A further step would be to incorporate an indicator in project evaluations that signals whether an equal amount of effort was spent on discovering citizen needs as on discovering new uses for technologies.

3) **Prepare well:** Add data protection clauses to procurement procedures and service agreements to better enforce GDPR requirements at the time when vendors still have an incentive to sign them. Collaboration between different municipalities, but also different departments, can help prepare smart city initiatives, for example through shared tools and templates for basic GDPR governance such as standard contractual clauses for joint controllership.

4) **Take advantage of the accountability principle:** The principle, in connection with transparency, affords means to control vendors, partnerships and simply to stay on top of things. Data Protection Impact Assessments (DPIA) are a useful tool in this context. Utilise them, make sure that they are not a one-off, but recurring at fixed intervals of your smart city initiatives. Conducting a DPIA only at the end of the decision-making, it is likely too late to make changes in technology. If done well, it can even function to involve stakeholders, give a voice to citizens, and ultimately to shape smart cities.

## VII. Conclusion

We applied a social constructivist approach to personal data protection in smart city initiatives. Based on the SCOT framework and a Quasi-Empirical Scenario analysis, the approach sheds light on interdependent interests, interpretations and influences of the four relevant groups. In addition, it underlines that smart city decision-makers should understand how context and technology steer towards particular choices in personal data protection and ask themselves what is socially beneficial, instead of what is legally safe or technologically most efficient.

This article is a starting point in analysing the social construction of personal data protection in smart cities. In more extensive analyses in future studies, subdivisions of these broad groups must be added. The meanings that smart city initiatives have for subgroups of citizens, for example, depend on their level of involvement or digital literacy and might differ substantially. Future research will also need to investigate appropriate means to raise literacy, skills, and capabilities of public administrators and public organisations, in order for them to understand the personal data protection requirements and apply them in the interest of their municipality.

An important aspect that the analysis has reinforced is that, in this stage of 'interpretative flexibility', the role of citizens is often diminished for one reason or another. We believe that the GDPR, its requirements and data subject rights, can become a vehicle to strengthen that role. Several research trajectories are investigating this aspect (the SPECTRE project is a leading example in this regard) and, perhaps, the time is ripe for constructing a privacy-aware, personal data protecting smart city that satisfies the needs of the citizens as much as those of leading technology vendors.

## Acknowledgements

This analysis was made possible by several research projects and initiatives funded by the Flemish region and the

[5] A recent example is the partnership between the German police and Amazon, which got plenty of attention in the media: all data captured by the police's 'body cams', including personal and potentially very sensitive data, was stored and processed on Amazon servers.

[6] Data ownership, though, is a legally debatable concept.

[7] imec-SMIT has been involved in several smart city related living labs, e.g. in course of the European research project ECIM. (ec.europa.eu/ecim-project)

European Union. These include the SPECTRE project (spectreproject.be), the Smart Flanders project (smart.flanders.be), the Select For Cities project (select4cities.eu) and the Antwerp pilot of the Synchronicity project (synchronicity-iot.eu/project/antwerp), in all of which is imec-SMIT leading partner. imec-SMIT is also strongly involved in the ESSENCE project (imec-int.com/essence) and the City of Things initiative in Antwerp (imec-int.com/en/cityofthings). Last but not least, imec-SMIT coordinates a VUB research chair on 'Data Protection on The Ground', in collaboration with the research group LSTS (Law, Science Technology & Society), and supported by BNP Paribas Fortis (vub.ac.be/leerstoel/dataprotection-on-the-ground) .

## REFERENCES

[1] S. Van der Graaf, 'In Waze We Trust: Algorithmic Governance of the Public Sphere', *Media Commun.*, vol. 6, no. 4, p. 153, Dec. 2018.

[2] H. Chourabi *et al.*, 'Understanding Smart Cities: An Integrative Framework', in *2012 45th Hawaii International Conference on System Sciences*, Maui, HI, USA, 2012, pp. 2289–2297.

[3] P. Ballon, *Smart cities: hoe technologie onze steden leefbaar houdt en slimmer maakt*. Leuven, België: LannooCampus, 2016.

[4] E. G. Carayannis and D. F. J. Campbell, '"Mode 3" and "Quadruple Helix": toward a 21st century fractal innovation ecosystem', *Int. J. Technol. Manag.*, vol. 46, no. 3/4, p. 201, 2009.

[5] I. Calzada and C. Cobo, 'Unplugging: Deconstructing the Smart City', *J. Urban Technol.*, vol. 22, no. 1, pp. 23–43, Jan. 2015.

[6] R. Kitchin, 'The real-time city? Big data and smart urbanism', *GeoJournal*, vol. 79, no. 1, pp. 1–14, Feb. 2014.

[7] A. Greenfield, *Against the smart city (The city is here for you to use)*. New York: Amazon Media, 2013.

[8] A. Townsend, *Smart cities: big data, civic hackers, and the quest for a new utopia*. New York, NY: W.W. Norton & Company, 2013.

[9] S. Sismondo, 'Science and Technology Studies and an Engaged Program', in *The Handbook of Science and Technology Studies*, 2008, pp. 13–31.

[10] T. Gillespie, P. J. Boczkowski, and K. A. Foot, Eds., 'Introduction', in *Media technologies: essays on communication, materiality, and society*, Cambridge, Massachusetts: The MIT Press, 2014, pp. 1–17.

[11] L. A. Lievrouw and S. Livingstone, 'Introduction to the Updated Student Edition', in *Handbook of New Media: Social Shaping and Social Consequences of ICTs, Updated Student Edition*, 1 Oliver's Yard, 55 City Road, London EC1Y 1SP United Kingdom: SAGE Publications Ltd, 2006, pp. 1–14.

[12] J.-C. Plantin, C. Lagoze, P. N. Edwards, and C. Sandvig, 'Infrastructure studies meet platform studies in the age of Google and Facebook', *New Media Soc.*, vol. 20, no. 1, pp. 293–310, Jan. 2018.

[13] T. J. Pinch and W. E. Bijker, 'The Social Construction of Facts and Artefacts: or How the Sociology of Science and the Sociology of Technology might Benefit Each Other', *Soc. Stud. Sci.*, vol. 14, no. 3, pp. 399–441, Aug. 1984.

[14] S. Jasanoff, 'Technologies of Humility: Citizen Participation in Governing Science', in *Wozu Experten?*, A. Bogner and H. Torgersen, Eds. Wiesbaden: VS Verlag für Sozialwissenschaften, 2005, pp. 370–389.

[15] B. Latour, 'Where are the missing masses? Sociology of a few mundane artefacts.', in *Shaping technology/building society: studies in sociotechnical change*, Nachdr., W. E. Bijker and J. Law, Eds. Cambridge, Mass.: MIT Press, 1992.

[16] R. Clarke, 'Quasi-Empirical Scenario Analysis and Its Application to Big Data Quality', p. 20, 2015.

[17] M. Godet, *Strategic Foresight/La Prospective - Use and Misuse of Scenario Building*. Paris: Cahier du LIPSOR, 2008.

[18] L. Moerel and C. Prins, 'Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things', *SSRN Electron. J.*, 2016.

[19] I. Kamara and P. De Hert, 'Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach', Brussels Privacy Hub Working Paper, 2018, vol. 4.

[20] F. Bieker, M. Friedewald, M. Hansen, H. Obersteller, and M. Rost, 'A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation', in *Privacy Technologies and Policy, Apf 2016*, vol. 9857, S. Schiffner, J. Serna, D. Ikonomou, and K. Rannenberg, Eds. Cham: Springer Int Publishing Ag, 2016, pp. 21–37.

[21] N. Ni Loideain, 'A Port in the Data-Sharing Storm: The GDPR and the Internet of Things', *SSRN Electron. J.*, 2018.

[22] L. Edwards, 'Privacy, Security and Data Protection in Smart Cities':, p. 32, 2018.