# SMART CITIES
## for city officials

A SOCIAL SCIENCES APPROACH

https://smartcitiesforcityofficials.com/

Smart Cities for City Officials- A Social Sciences Approach, 2021.

Editors:
Guy Baeten, Institute for Urban Research, Malmö University
Chiara Valli, Institute for Urban Research, Malmö University

Research assistant and graphic design:
Adriana de la Peña, Institute for Urban Research, Malmö University

Contributors:
Rob Kitchin, Maynooth University
Ola Söderström, University Of Neuchâtel
Bianca Wylie, Centre for International Governance Innovation

Published by the Institute for Urban Research at Malmö University
with support of FORMAS grant REF. 2017-01422.



https://smartcitiesforcityofficials.com/

# MODULE 4

## Big Data, Privacy and Security

*"Some of the most progressive work in terms of using data and technology in cities, is going to be about reverting, reducing and taking back public power of systems that are already highly privatised and highly problematic" (Bianca Wiley).*

*In this module we discuss some of the most controversial and most complicated questions that smart city projects can possibly raise: the collection and use of data, data privacy, data security, data ethics as part of broader government accountability.*

# Module 4
# Big Data, Privacy and Security

GUY BAETEN- In this module we will present expert opinions about the collection and use of data in the smart city. The issues of data privacy, data security, data ethics and the accountability of those actors collecting data belong to the most controversial and most complicated questions that smart city projects can possibly raise. Most people agree that data collection is the very business model behind smart cities. If we want to engage in smart city projects, we will have to accept that data collection will perhaps be the most central part of it, and that triggers controversies that we need to deal with whether we like it or not, and this module tries to help us find some answers to these controversies.
Questions around the collection and use of data include the question of whom can collect data. Can private actors collect data and use them for commercial purposes? Can public actors collect data and use them in certain ways or sell them to private actors?

CHIARA VALLI- What kind of data can be collected? Is it only data that can be immediately used for improving certain municipal services such as public transportation, or can other data be collected that have no immediate value for improving the quality of public services?

GUY BAETEN- Another big question is who will own the data? Will there be open data sources accessible for everyone or will data be stored on private servers? Will data collection guarantee the privacy of city dwellers or can stored data be traced back to individuals?

CHIARA VALLI- Will city dwellers need to give their consent to data collection and how can that possibly be organised? Do citizens know what data are being collected?

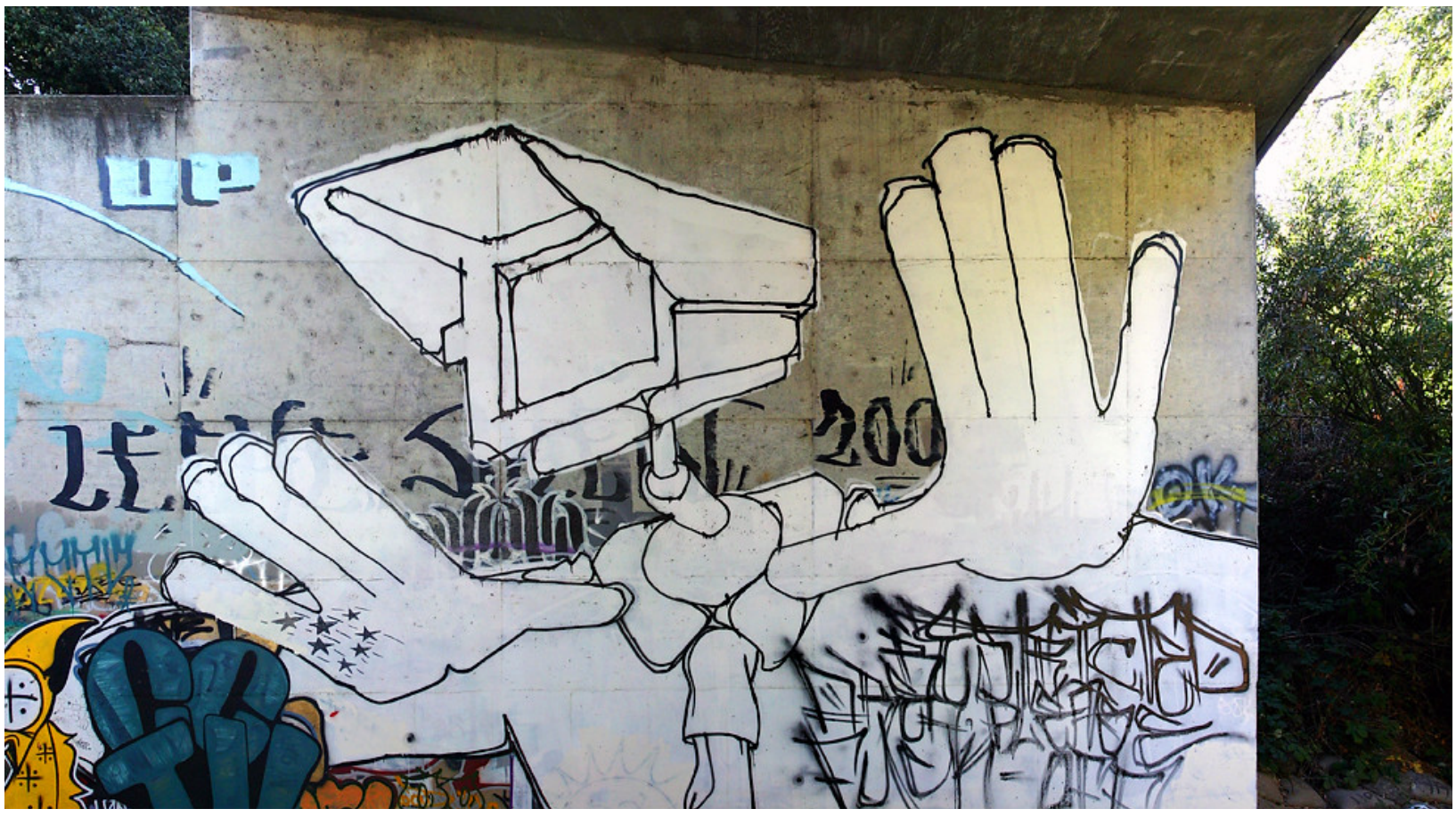
GUY BAETEN- These are just some of the questions that are continuously debated and that have no simple answers. Data collection in public is a relatively new phenomenon and is poorly regulated. That makes it all the more difficult for people working with smart city projects on a daily basis to make fair decisions regarding data collection, data storage and data use. And it opens up for experimentation since it is not obvious what could be best practice. In Toronto for example, where Google's sister company Sidewalk Labs tried to build a new smart city district where it would collect all sorts of data, a range of un-clarities around that data collection had triggered a very intense debate in the local media and beyond. Some people argued that publicly collected data should be publicly owned and not owned by a private company. Some people expressed their worries that collected data could be shared with third parties, companies who would try to sell them. Others raised issues about security: what if the functioning of your city becomes completely dependent on data and algorithms run and managed by a private company? What control mechanisms could exist if data collected in Canada are stored on US servers? What if the computer systems running your city are hacked? There were fears that the Google district in Toronto would become the first large-scale urban experiment in surveillance capitalism – making profit from collecting data about everyday urban life– and it is one of the main reasons why the project did not go ahead after protests from activists and business leaders alike.

CHIARA VALLI- Data collection in smart cities is in fact a highly infected debate with both citizens and municipal authorities expressing privacy concerns, security concerns and accountability concerns when smart city providers make known their desires to collect data in the city. The big question, then, is: how should, how could, cities, and city officials running those cities, be managing the collection, processing and use of data in the 21st century? There is no simple answer, but we have gathered some useful thoughts from some of the experts we interviewed.

We start with Rob Kitchin, who is one of the most prominent smart city researchers today. He has been an advisor to the Irish Government Data Forum where he made some recommendations for cities to manage and govern privacy and security issues. We asked him what Nordic cities could learn from that. He sees four organising principles to handle data privacy and security.

ROB KITCHIN - I basically mapped out four levels of solutions. The first one is the *market*. So, companies themselves self-regulate. There are industry standards, there are industry bodies that certify, or whatever. Or there's a notion of which there's ethics of competitive advantage. A company basically says, “I have better security “or “I have better privacy than other companies, move your business to me”. You try to make privacy a point of competition between companies.

The second level is *technological*, which is typically where a lot of funding and companies have been working, which is basically that you try to improve the security. You do end encryption, you do access control, security controls, audit, trails, backup, patching, all that kind of stuff. Or you have things like privacy enhancement tools that the public can use. Like on my Firefox browser, I've added blockers, and “http” everywhere, and Privacy Badger and so on. I got a bunch of plug-ins that are trying to enhance my privacy, the use a VPN, all that kind of stuff.



The third level is *policy and regulation*. We have things like the Fair Information Practice Principles introduced by the OECD in 1980. Kind of been undermined by big data, and basically just revisiting them and making sure that people understand the value of them and getting them reintroduced back into policy where they've kind of slipped out a bit. Promoting things like privacy by design, where privacy is baked in from the start, as opposed to things being open, and then you close down the privacy. Security by design, around things like education and training, to teach people what the risks are, how they can protect themselves and how they protect their organisation.

And the last level was *governance*, which is around things like the vision and strategy and having things like stakeholder advisory boards that can give direction about how the smart city might develop. Having things like oversight and compliance measures. A lot of public bodies would have risk governance boards to look at the organisational risk and make suggestions about procedures and so on that need to be put in place. But they also do oversight on that, and they do mitigation, preventative measures, and they do discipline the organisation to a certain degree.

And then in the last part of governance is really down at the day-to-day level, where you might have a privacy team within the organisation. A lot of American cities now have privacy impact teams, who will evaluate what's going on. Or you might have a computer emergency response team, which is basically what happens if your city is hacked. That is the security thing that is happening now with smart city technologies. Bits of transport infrastructure, or energy infrastructure are being hacked and taken offline. A whole load of American cities over the last couple of years have been hit with ransomware attacks, where better technology has been taken over and held to ransom and cities have had to pay a lot of money. A couple of cities literally went offline for a few days, while they tried to get that sorted out. And we should not get to do any more manual procedures. All the tacit knowledge is gone. Like if the technology disappears, they got a problem. Things like the Emergency Response Teams are really important.

They were our solutions: 1) market, 2) technological, 3) policy regulation, and 4) governance. The fifth one is obviously *legal*. And depending on which jurisdiction you're in, the legal thing will vary. Whether you have the competence around that will vary. And it will vary inside countries. Somewhere like Canada, it could vary at the local level, the federal, the state level. Same in the US.

CHIARA VALLI- So, Rob Kitchin discerns four mechanisms to improve the privacy and security of data collected in the city with the help of smart city devises: first, competition between companies to provide data collection that respects privacy and security. Second, technological instruments to enhance security and privacy. Third, regulation like we have now through the GDPR for example. And finally, governance that works with visions, strategies, advisory boards in order to create oversight when implementing smart city projects.

GUY BAETEN- For Bianca Wylie the question of data collection and data use should be placed in the wider context of what cities should do more generally at this point in time. Bianca Wylie is the most prominent critic of the Sidewalk Labs project in Toronto. She has been appearing in media very regularly and has been writing a lot of opinion pieces about Google's plans for Toronto. She has been called the "Jane Jacobs of smart cities".

Jane Jacobs was the urban activist who was fighting Robert Moses' plans for highway construction and demolition in Manhattan back in the 1950s and 1960s. Jane Jacobs was taking on the American Goliath of urban development so to speak, and now we see Bianca Wylie taking on Google, so the comparison is obvious. Bianca Wylie believes that we should do more than simply talk about the management of data collection and the use of data to make planning decisions. For her the question is much broader: the fundamental question is how we use technology in local government, and how cities can be stewards of public infrastructures, and how we can use technology, including data, to make cities stronger and make them do better what they have been good at for a long time. We should not reinvent cities, but we should reinforce cities says Bianca Wylie.

BIANCA WYLIE- One thing that cities are obligated to do in this moment, is to use their role as stewards of public assets- public infrastructures- and to move away from thinking about data as some sort of inherently useful commodity, and return to accountability and professionalism in terms of decision making. And they need to go back to using software, using hardware, using technology to grow what they've already been doing well for a very long time.

I think we really have several intersecting crises here. Cities and the governance in cities need to be reinforced, not reinvented. I think that's of critical importance. And in there we have some nested problems. Urbanism, for example, is an inherently technocratic undertaking. It has been a long standing violent, racist undertaking. So, a lot of the issues that have been raised from a technology perspective were already inherent to the city as a construct. So, the reason it's so good to be thinking about this more from sociology and other lenses, is to question, how do we build the confidence back in the governance that we have in democracy? Those issues are of much more relevance than anything that's really highly technical.

Data has become that unquestioned handle that people grab to say, "we need to democratise the data", "we need to better utilise the data", or "the data is important for this economy". The reality is, we need to think about the technology, and I think infrastructure is not as easy a word to grab as data. But it's the software, generally speaking, where our accountability issues are sitting right now, and they have been, and software has been outsourced for numerous decades. So, we need to advance the conversation into questioning how technology is used in local government.

Those are high level thoughts, but I know there is a lot of little pieces that I know we can get into.

CHIARA VALLI- Bianca Wylie puts into question our data collection practices. Regulation and governance are important but there is more to it. A lot of data is being collected without consent. She is convinced that we have to revert and reduce data collection, rather than increase it if cities want to take back public power over technological systems. She understands that cities are under pressure to become 'smart' since that is the latest trend in local economic development, but the issue is broader than just developing systems that respect individual privacy and security. The issue is more than just gaining individuals' consent for the use of their data. The issue is infrastructural security: how can we make sure the infrastructures we put in place are safe and secure from attack? That is a point Rob Kitchin also touched upon when he talks about the governance of smart cities.

BIANCA WYLIE- The simplest answer for me with data, security, privacy, everything out says: Don't have it. Don't collect it. If you are a local government, you should be thinking defensively about why you want to be holding this liability. You really should. And I think this is where we have a bit of a pro and con with the security industry saying: "sell cities on fear." And that's why so much of the infrastructure has been already outsourced. So strategically, cities need to think about the fact that you can't outsource government accountability. And that is only one type of risk. People who deeply understand security, understand that the best security is to not have the data in the first place.

**"People who deeply understand security, understand that the best security is to not have the data in the first place."**

That should turn the amount of attention to questioning, what do we really need to hold? And, again, let's go back to the idea that this is hard to do when there's pressure to be collecting data as an input to an economic development program. I understand the tension there. But if you turn your neck to the tables that are looking at national security, at military application of artificial intelligence, at how technology and national security come together, one of the areas of concern is infrastructure. The kinds of infrastructures that are potentially open to attack because they are connected to technology systems. That is an issue that is being pushed by the industry very clearly. But it is also real. And we need to think about what a local-national relationship looks like in terms of managing and protecting assets, if there is going to be a technological layer. And that's different than privacy. This is not about personal security. This is about infrastructural security and asset management. That, I think, is a granular differentiation that needs its own strategy. And given the financial assets that cities have to manage things like that, there probably needs to be regional and national cooperation that's going on at a different level than today.

**"To pretend there is some kind of model to create symmetry between resident power, and technological power, or even municipal power, as though there is a level field, it's not true. And that's not real. From a democracy perspective, consent to me is not useful."**

Now, if we want to go back over to privacy, consent is absolutely not a construct that anybody should be pretending has carriage right now. And anyone who wants to keep talking about consent, I don't take it seriously. Because that model, for so many different reasons, isn't working. You can't opt in and opt out of things happening at a collective municipal level. It's like another urban planning problem, who shows up to the local meetings about how the neighbourhood develops? White landowners. Who shows up to the meetings about how data use is going to go on? How many people are really set up to come in and participate in their data wallet? Let's not pretend that that's the entire population. That is, at a very high level, critical to understand for democracy and data use.

But at a secondary level, we have to think about the fact that synthetic data is something that is on the table for cities. That they're talking about making digital twins. We're at the point now, where companies are saying that we don't really need to use anyone's particular data, that this is just like a profile. And this is already happening all over the place. It doesn't need to be your data for you to be discriminated against. And again, we

know this from things like postal codes. This is not new, none of this is new. So, to pretend there is some kind of model to create symmetry between resident power, and technological power, or even municipal power, as though there is a level field, it's not true. And that's not real. From a democracy perspective, consent to me is not useful. And this is why we have to question, what do cities already have mandate from residents to do with information? That should be a very prominent piece of rationale for using any kind of data. But secondarily, are you ready as a city to stop doing things that you've been doing for years already, where you never got consent? Because we need to remember there is a major deficit of what cities are already doing, and what the public knows is going on.

> "Some of the most progressive work in terms of using data and technology in cities, is going to be about *reverting, reducing and taking back* public power of systems that are already highly privatised and highly problematic."

So, I think I'll stop here by saying: people right now really need to zoom out in the timescale and understand that some of the most progressive work in terms of using data and technology in cities, is going to be about *reverting, reducing and taking back* public power of systems that are already highly privatised and highly problematic.  And that's where open government is in an interesting moment.

There is fairly recent, fairly under-utilised, mostly public relations conversations about this reduction and minimisation of technology. If governments want to be taken seriously right now, they need to rip the veil off to see what's going on and figure out a way forward. But that way forward is not creating new complexity, it's actually, in some cases, removing some of the infrastructures that exist and re-examine core functions. And what might help this to happen is the financial pressure cities are under.

We don't have time for all of these layers of technology that, quite frankly, don't even have efficacy. Efficacy should be the number one thing when you're looking at operations in a municipal context. If you look at all these disjointed systems, you don't even know what's going on. You've got risks flying all over. It's unclear if they're working and the public doesn't know what's going on. Let's not pretend that now in 2021, we're are going to figure out how to depart from here like things are fine. They're not fine at all. And that's a shared burden.

I've gone in a few different directions. But I think at the core of it we know that consent is not a model that is useful. And we need to figure out how to do accountable use of technology. And accountability is the one word that should be in the front. How do you explain what you're doing? Because that's always been what governments have to do: You do a thing, there's always some risk, there's always some issue, there's always going to be a way that something gets misused. So, how will residents hold you accountable for the use of their data and the use of public technology? That's the question that should be flying through every process right now. Accountability, not privacy.

I think a lot of us understand why privacy is important. But if you are shifting these things out of public control, you lose accountability. That's why, as a fundamental piece of these debate, when people hear the words privacy and security, we need to rethink what does

security really mean, and where does privacy fit into the broader set of issues that governments need to be held responsible for.

GUY BAETEN- So for Bianca Wylie there are much wider issues at stake than simply data collection regulations and governance. That is an opinion shared by Ola Söderström. Ola Söderström has been writing some key academic texts about smart cities. For Ola Söderström, the issue is data sovereignty. Those who have sovereignty over something, for example data, possess ultimate power and are free from external control. Sovereignty over data used to be in the hands of public authorities, nation states, but this power has now shifted to private actors. This means not only that public actors have lost their sovereignty over data but also individuals have lost sovereignty since they don't know what data are being collected, how they are processes and how they are used. This is how Ola Söderström formulates it:

OLA SÖDERSTRÖM- There are many things to be said about how platform companies shape our uses of the city, or choices, or our consumption decisions. But one point, I think, is more general and important: with platform companies, the main effect is the effect on what I would call *data sovereignty*. So, if we look at the history of statistics with William Petty in the 17th century in Great Britain, we know that for 300 years since the beginning of statistics, it's been about a state monopoly. Statistics etymologically refer to data for and by the state. What's been happening in the digital age is the erosion of the state of sovereignty. And this has been very much increased in the past 10 years with the rise of digital platforms.

"The state is no longer the institution with the most precise data about issues like mobility, housing, or consumption. And I think this can be quite worrying."

So you have a situation where you have the companies mentioned Airbnb, Uber and Google, who have a huge amount of urban data, which they extract from the traces we leave in our practices, and traces that as we know, and we know it especially from Shoshana Zuboff brilliant work on surveillance capitalism, there is what she calls *behaviour surplus*, i.e. the kind of traces we leave which are not necessary for the services of the company itself. This is what is the main assets of the digital platforms. And this is what is sold. And this is what is the main purpose of Google friends list.

So the important questions around these effects is firstly, *extraction and commodification of our personal data*. And this concerns our private daily lives. And this is done in very opaque ways. We don't know about the use of data, or we consent to them in the ways we know we consent to them: you tick a box because you are just bored about the two pages of things you get from whatever platform. So that's the first problem - the extraction and commodification of our private data.

The second thing is *the gap between publicly owned and privately owned data*. So, the state is no longer the institution with the most precise data about issues like mobility, housing, or consumption. And I think this can be quite worrying.

And the third related problem is *the lack of access to data*. We know that digital platforms, they ask of us to be very transparent, but they are very opaque about what they do with the data, and how their algorithms actually work. It means that these companies are very difficult to regulate. Without access to Airbnb's data, it's very difficult to regulate the short

term rental markets when you decide to do so. Many cities do not decide to do so, but beginning to decide to do so is very difficult. So, I think these effects are very profound. And we need to talk about this when we talk about solutions. But they are things to be done in that respect.

GUY BAETEN- Talking about surveillance capitalism, there are quite a few people who argue that surveillance is the very business model of smart cities, and raises all kinds of issues of ethics, privacy, security. Would there be a smart city that has not surveillance at its central core and data generation? And how would that differ between, again, global north and south? If there are any differences?

OLA SÖDERSTRÖM- In Cape Town, there is an interesting civil society organisation called the Social Justice Coalition, and some of my colleagues have been writing about Social Justice Coalition. And they play an important role in what I call "data politics" in Cape Town. And Social Justice Coalition has calculated the rate, the number of policewomen and policemen per 1000, inhabitants for different areas of the city. They came to the conclusion that there are much more police forces in the affluent areas of Cape Town, compared to the townships and informal areas - the so-called Cape flats- while the rate of crime is much higher in the Cape flats.

There is an issue here of access to safety. There's an issue here of distribution of safety forces. And this is, of course a political decision. And what I found very striking in terms of how these questions can be framed differently in different places in a very coherent way. The Social Justice Coalition asks for more police forces in the informal settlements and in the townships. And, thinking about this, would that happen in Switzerland, in Sweden? Would that happen in the favelas in Rio when you know what policing means in the favelas? Certainly not.

The way safety is framed, what surveillance means in different contexts for different populations is quite different. But having said this, I think your point is important. Paolo Cardullo recently wrote a very nice book, entitled Citizens and the Smart City. He has a

nice way of technically saying, there's a totalitarian affordance in the smart city, which means the smart it is not totalitarian, but the way it is framed. It's so much about capturing data, collecting data, there is something which goes in the direction of authoritarian governmentality. I think the issue here is not so much about distinguishing between the global north and the global south again, but distinguishing between semi authoritarian or authoritarian governments and democratic ones. Because these are the government's- the authoritarians ones- which will use the totalitarian affordances of the capacity to surveil people in their everyday lives, in the minutiae of their everyday lives.

And if you think about what has been happening in India with the Modi regime, the checks and balances in countries like Sweden and Switzerland, would not allow this to happen, at least for the time being, with the governments we have. It might change.

There are a series of very important radical issues here about data and surveillance, because there's so much knowledge about the whereabouts, where we are, what we do. So, the balance between safety and privacy is a crucial question in the smart city, for local governments, regarding state control data, but also regarding data produced and stored by private companies.

GUY BAETEN- Ok, now we have heard some thoughts and reflections from the people we interviewed about data collection, data processing and data use in smart cities. Many interesting points were made but the main thought I take home from listening to these interview clips is that data safety and security should be understood in a broader context than just regulation and governance, even if they are very important too. Cities may want to reflect more on how to use technology, and that would include smart devices that collect data, to do better what they are already good at. Smart technology should support the city's existing services and infrastructures, rather than being an instrument to replace the public authority of cities with private authorities. It is the issue of data sovereignty that is at stake here: cities should be careful not to give away their data sovereignty to private actors but should keep control over it and remain accountable to the public.

I think all the experts agree that we need more basic reflections on the use of technology in the city and that it should be transparent for citizens what smart technologies, data collection and use is being implemented by the city. That brings us to the topic of the next module. In the next module, we present the thoughts of our interviewed experts on the issues of participation and democracy.

## REFERENCES


Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (1st edition). PublicAffairs 5(4), 216–224.

Cardullo, P. (2020). Citizens in the 'Smart City': Participation, Co-production, Governance.

*Social Justice Coalition- Home*. (n.d.). Retrieved August 26, 2021, from https://sjc.org.za/