

decode

Reclaiming the Smart City

Personal data, trust and the new commons

July 2018



DISCLAIMER By the European Commission, Directorate-General of Communications Networks, Content & Technology. The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

© European Union, 2018. All rights reserved. Certain parts are licensed under conditions to the EU.

Reproduction is authorised provided the source is acknowledged.

This work is licensed under a Creative Commons AttributionNonCommercial -ShareAlike 4.0 International License



Authors

Theo Bass, Emma Sutherland and Tom Symons (Nesta)

Reviewers and contributors

Francesca Bria (BCN IMI), **Oleguer Sagarra Pascual** (BCN IMI), **Gijs Boerwinkel** (Waag), **Job Spierings** (Waag), **Stefano Bocconi** (Waag), **Stefano Lucarelli** (CNRS)

Project partners

BCMI Labs AB, City of Amsterdam, CNRS, Dyne.org, Eurecat, Technology and Digital innovation Office, Barcelona City Hall (IMI), Nesta, Open University of Catalonia, Politecnico di Torino/Nexa, Stichting Katholieke Universiteit Nijmegen Privacy & Identity Lab, Thingful, Thoughtworks Ltd., UCL, Waag.

Acknowledgements

This report was made possible thanks to the support of a number of people. The comments of our reviewers in earlier versions were invaluable in helping to shape the final outcome: **Francesca Bria, Oleguer Sagarra, Gijs Boerwinkel, Job Spierings, Stefano Bocconi** and **Stefano Lucarelli**.

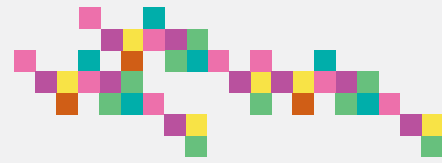
We would also like to thank all of those who gave up their time to speak with us about the projects which they are involved with: **Aik van Eemeren, Berent Daan, Caroline Nevejan, Dolfi Mueller, Ger Baron, Guillem Camprodon, Jordi Cirera, Karl-Filip Coenegrachts, Malcom Bain, Mara Balestrini, Mariona Ciller, Màrius Boada, Nanette Schippers, Ruurd Priester, Theo Veltman, Willem Koeman, Wouter Meys, Xavi Roca, Zach Hecht**.

Also thank you to **John Davies, Juliet Grant, Tom Saunders, Chris Haley** and **Eddie Copeland** at Nesta who have helped steer this report and provided useful comments on earlier drafts.



Contents

<u>Executive summary</u>	4
<u>Introduction</u>	6
<hr/>	
<u>Section 1: Smart cities, data and ethical challenges</u>	9
<hr/>	
<u>Section 2: Policies for more responsible innovation with data in cities</u>	15
<u>Leader</u>	20
<u>Guardian</u>	24
<u>Catalyst</u>	28
<u>Provider</u>	32
<u>Connector</u>	38
<hr/>	
<u>Section 3: Lessons for city governments</u>	44
<hr/>	
<u>Appendix 1: Case studies</u>	47
<u>Appendix 2: DECODE Barcelona Pilots</u>	60
<u>Appendix 3: DECODE Amsterdam Pilots</u>	61
<u>Appendix 4: DECODE Pilot Evaluation Methods</u>	63
<hr/>	
End Notes	65



Executive summary

This report is about why and how city governments are taking a more responsible approach to the use of personal data. It addresses some of the major flaws in how traditional smart city projects have approached data collection and use. It then provides a summary of policy roles available to local authorities to address these challenges. The report is based on case study research of a range of pioneering examples of city governments around the world that are trying to rethink how they collect, analyse and use data collected about people, and concludes with a set of eight lessons for how others can learn from these approaches. This report is part of DECODE (DEcentralised Citizen Owned Data Ecosystems), a major EU Horizon 2020 project which is developing practical tools to give people control over how personal data is used, and the ability to share it on their terms.

Cities are becoming a major focal point in the personal data economy. In city governments, there is a clamour for data-informed approaches to everything from waste management, public transport through to policing and emergency response. In the context of rising demand and expectations, and in many cases decreasing budgets, it now seems inconceivable that these pressures can be managed without getting more value from the vast quantities of data available to city governments. For the private sector, the city also represents a key source of data collection and use. From sharing economy platforms such as Uber or Airbnb, to providers of the technology that power local services, cities are a crucial setting for collection of the data that enables modern tech firms to thrive.

While better use of data by governments brings opportunities for citizens - personalisation, efficiency, more timely and easier interactions - there are also new risks. This report identifies three key challenges from the increasing use of data in the running of city governments:

- Traditional notions of ‘smart city’ put individual privacy at risk. Cities want to be connected, and data-driven, but in doing this many are unwittingly engaging in large-scale surveillance of citizens.
- People have little say over how their personal data gets collected and used, and there are few options that allow policymakers to acquire people’s data in a more consent-driven way.
- While dominant internet business models encourage stark new imbalances of power, city governments are unsure how to play a more active role in leveraging more responsible innovation with data in the local economy.

The nature of this debate can sometimes suggest that these objectives - privacy and personal control on the one side, the use of data for smartness and efficiency on the other - are in conflict. It is a central argument of this report that this framing is unhelpful and that these two objectives do not have to be in conflict. This report therefore explores how cities can make them mutually compatible, through policy choices and through new technologies.

This report brings together a range of case studies featuring cities which have pioneered innovative practices and policies around the responsible use of citizens' data. Our methods combined desk research and over 20 interviews with city administrators in a number of cities across the world. We translate the policies and projects from our case studies into a summary of policy roles. The five policy roles we identify are:

- **Leader** - How is the city setting a clear direction for change, while creating the internal capability to support a more responsible and privacy-preserving smart-city agenda?
- **Guardian** - How does the city create rules to protect people from harm caused by digital tools, and ensure that the use of innovative new data-driven technologies is able to benefit everyone?
- **Catalyst** - How is the city leveraging its buying power to create new incentives and encourage more responsible innovation in the wider economy?
- **Provider** - How is the city becoming a test-bed for new tools and services that respect each person's right to privacy and promote greater individual control over personal data?
- **Connector** - How does the city collect and use personal data in a way that fosters high quality and consent-driven engagement with citizens?

Based on our case studies, we also compile a range of lessons that policymakers can use to build an alternative version to the smart city - one which promotes ethical data collection practices and responsible innovation with new technologies.

1. Build consensus around clear ethical principles, and translate them into practical policies
2. Train public sector staff in how to assess the benefits and risks of smart technologies
3. Look outside the council for expertise and partnerships, including with other city governments
4. Find and articulate the benefits of privacy and digital ethics to multiple stakeholders
5. Become a test-bed for new services that give people more privacy and control.
6. Make time and resources available for genuine public engagement on the use of surveillance technologies
7. Build digital literacy and make complex or opaque systems more understandable and accountable.
8. Find opportunities to involve citizens in the process of data collection and analysis from start to finish.

This report is aimed at policymakers and practitioners in city governments and local authorities. It is written to support the DECODE project, which aims to create a new set of technical platforms that let people decide whether to keep personal data private or share it for the public good. DECODE works with city governments, researchers and social innovators to discover how giving people more control over personal information online can enable new forms of value to emerge from data - new types of 'commons' for personal data. However, despite being a highly technical project, this vision cannot be achieved with technology alone. There has to be the backing of the city administration, and a policy framework which is supportive to giving users greater control and privacy. This report aims to stimulate and support the development of such policies in cities across the world.

More broadly, it aims to provide a source of inspiration and ideas for city governments looking ahead at a data-driven future. Many are already taking proactive steps to ensure that the benefits of data-informed government do not come at the expense of their citizens' privacy. This report is designed to help others move in the same direction.



Introduction

This report is about why and how cities are taking a more responsible approach to how they use data.

Around the world, cities have become the focal point for the rapid growth in the production and consumption of data, from smart city programmes, government data analytics, and organisations in the private and social sectors who are all hungry to integrate data to enhance performance.

This is a triumph for advocates of the better use of data in how we run cities. After years of making the case, there is now a general acceptance that social, economic and environmental pressures can be better responded to by harnessing data. But as that argument is won, a fresh debate is bubbling up under the surface of the glossy prospectus of the smart city: who decides what we do with all this data, and how do we ensure that its generation and use does not result in discrimination, exclusion and the erosion of privacy for citizens?

These two questions have taken on particular significance in recent years as smart city programmes have integrated personal data alongside sensor data such as air quality, bus movements or traffic levels. Smart city projects are now tackling issues such as violence in town centres, burglary prevention, administering parking tickets, and reward systems for environmentally or socially positive behaviour.

It is perhaps curious, then, that privacy has tended to be a low ranking concern for companies and governments embarking on smart city programmes. While privacy campaigners have been warning of the risks these programmes present for years, it is only recently that this has begun to register as a mainstream concern. In some instances, conversations are recorded, a person's movements are tracked in granular detail, and facial recognition is used with static and mobile cameras. This data paints an extraordinarily intimate picture of people, often without them even realising.

The most obvious challenge is that the value of data grows the more it is linked, but this also increases the risks of identifying people or uncovering private information. Data-driven services have the potential to deliver massive efficiencies, as well as making our lives easier - from merging and matching data from different sources to predict illness, to providing insights into products or recommendations. Yet, these same efficiencies may come at the cost of our privacy. With this tension, city governments are quickly approaching a crossroads, where on the one hand data can make services significantly more personalised and useful, but on the other companies and policymakers risk causing severe discomfort among people who have little control or understanding about how those insights are being derived.

The nature of this debate can sometimes suggest that these objectives - privacy and personal control on the one side, the use of data for smartness and efficiency on the other - are in conflict. It is a central argument of this report that this framing is unhelpful and that these two objectives do not have to be in conflict. This report therefore explores how cities can make them mutually compatible, through policy choices and through the use of new technologies.

This report is focused on city governments. Traditionally data protection issues are dealt with by lawmakers at the national and European level. However, there are three reasons why we treat cities as the subject of this report:

- **Cities are emerging as new battlegrounds over personal data.** As cities hold concentrations of people, the growth of personal data has inevitably led to cities becoming central to the data economy. Over recent months and years, city governments have become important actors in shaping the data economy, from creating ‘smart’ urban environments to actively playing a role in the regulation of data-driven platform giants like Uber and AirBnb.
- **Cities are closer to the lives of everyday people.** Cities cannot solve all of our digital problems, but they can run smart, data-intensive public transportation, housing, health and other public services which millions of people interact with every day.¹ Being closer to people, cities are also better able to partner with local community and advocacy groups, pilot new technologies and consult with the public on their implementation.
- **City governments are often more flexible than regional or national governments.** Although data protection frameworks are usually enforced by higher levels of government, cities will play an important role in creating pressures and testing new standards from below. They are more flexible and are in a better position to experiment with new policies and technologies in a contained, local environment.
- **Cities are often the most appropriate focus for entrepreneurial ecosystems.** The most connections, skills, resources and finance tend to be sourced at city level, making them an optimal place to develop and trial new technologies which require an ecosystem to link to.

Purpose and outline of this report

This report is part of the DECODE project, part of the European Union’s Horizon 2020 programme. It is an ambitious three-year multi-disciplinary Innovation and Research Action project with the aim of giving people more control over personal data. The technology developed in this programme combines advanced in cryptography and distributed ledger technologyⁱ to create tools which give people user-friendly, granular control over personal data, including the option to share it for public benefit.

This technology will be piloted at the city level, in Barcelona and Amsterdam, which are recognised as two cities that are leading in combining grassroots movements and communities with the smart city agenda. The pilots focus on real-world problems in these two cities where the need for greater individual control of data has been recognised, such as participation in digital democracy, participatory citizen sensing and the sharing economy.

The technology of DECODE is just one part of these pilots. The project seeks to create a ‘commons’ⁱⁱ of citizen generated data which can be used by city governments, innovators, researchers and citizens alike. Such technology cannot be implemented in isolation. For DECODE to achieve its vision, there has to be the backing of the city administration, and a set of policies which are supportive of giving users greater control and digital privacy. For DECODE to be successful, in pilot stage and later on if it scales to other cities, aligning these policy and contextual factors with the deployment of the technology will be an important part of this success.

i. A distributed ledger is a type of database which is spread across a network of computers, known as nodes, which is not controlled by any single actor and is immutable.

ii. A shared resource belonging to, and governed by, a community of peers.



This report sets out the policy implications of running DECODE in a city government context. Our starting point is therefore in-depth case study research centred on Amsterdam and Barcelona. As two cities selected for their ability to be a test-bed for DECODE, an investigation into their recent history as leading smart cities, their policy development and their local contexts provides valuable insights to other cities. In scoping out this research we found that a select number of other cities share a common view, and are also setting high standards on related policy initiatives. By bringing these cities into our research, our aim was to create a more complete picture of the different policy roles and actions available to local policymakers which help them to take a more responsible approach to data-driven innovation.

The following report is structured into three sections.

- The first section addresses ‘why’ current trends in data collection and use are a problem that city-based policymakers need to respond to.
- The second section provides an overview of the case study research: the ‘what’. We give an overview of our method, before presenting a range of policy options performed by local governments around the world.
- The third section offers a summary of lessons - the ‘how’ - learning from our case study research.

The DECODE project: Unlocking the value of data as a common good

For many years it’s been a cliché to claim that information or data are the new oil. This fits well for the purposes of commodifying and selling data, but the analogy poorly matches data’s core properties. Oil is a scarce physical resource. Data and information by contrast can be replicated without limit and often become more valuable the more they are shared.

But unlike, say, open data, personal data generates tensions that can be difficult to reconcile. While personal data needs to be shared, aggregated and analysed to provide value, there are considerable risks to sharing it too. These include data falling into the wrong hands, or revealing more about us than we are comfortable with. DECODE responds to this challenge by creating tools that allow people to set fine-grained terms of use for data, flipping the current terms and conditions model on its head. By giving users the confidence that the data they share will only be used by the people they intended it to, DECODE aims to enable a whole ecosystem of value to be built on top of this data, which the project calls the ‘data commons’. In order to achieve these goals, the project will develop and test the following:

Flexible rules to give people full control: There is currently a lack of technical and legal norms that would allow people to control and share data on their own terms. If this were possible, then people might be able to share personal data for the public good, or publish it as anonymised open data under

specific conditions, or for specific use-cases (say, non-commercial purposes). For this DECODE is using a combination of Attribute-Based Credentials and distributed ledger technology to build a system of ‘Smart Rules’ which are flexible licenses that allow people to attach specific permissions to personal data. These are the foundational protocols on top of which all DECODE applications will be built.

Trusted platforms to realise the collective value of data: Much of the opportunity for sharing will only be realised where individuals are able to pool their data together to leverage its collective value. DECODE is working with platform cooperatives like GebiedOnline, and other communities like Decidim (Barcelona’s digital democracy portal) to provide a testing-ground where personal data can be shared for specific purposes decided by the participants.

Community-building in two pilot cities: DECODE is partnered with Barcelona and Amsterdam city councils where there are links to active digital social innovation communities across the two cities. For example, in Barcelona the project will bring together the council and the Making Sense project to assist local communities with new forms of citizen sensing. This kind of activity will be accompanied by a range of other external events, including hackathons and challenge prizes, meetups, a summer school and large-scale conferences to engage a range of different stakeholders and raise awareness about the pilots.

Section 1

Smart cities, data and ethical challenges

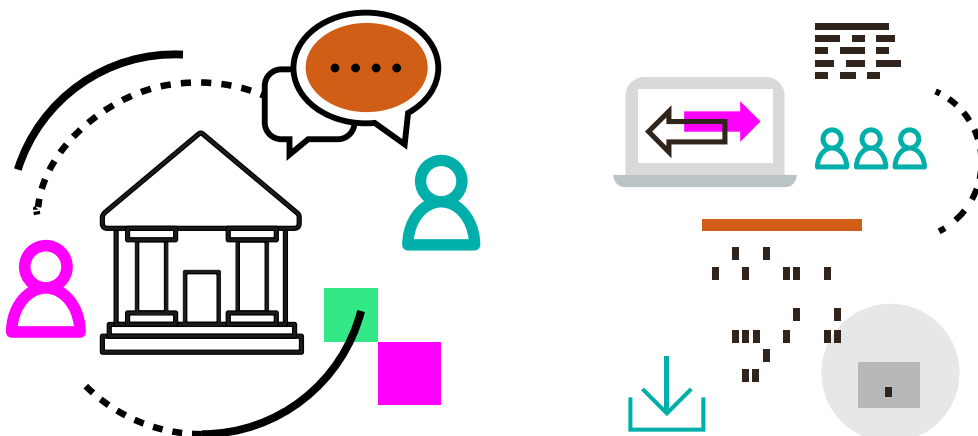
Many city governments have been keen to adopt the smart city mantle.² These cities invariably point to new technology and big data as a means of optimising the running of a government or place. Powerful, data-intensive technologies like Internet of Things (IoT) and artificial intelligence (AI) are becoming more integrated into the operation of public spaces. Faced with growing scale and density, the aim of increased data collection is better local policymaking: to measure crowds, optimise public transport, manage traffic and pollution, inform planning, monitor crime and much more besides.

Perhaps one of the biggest incentives for cities becoming 'smart' has been the opportunities this brings for economic development - local companies can harness the city's advanced infrastructure to develop sophisticated technologies for cities around the world. An element of prestige is also tied to this - political leaders want their cities to rise up smart city rankings; they believe that smart cities will be attractive places for people and businesses to move to.³

For many years it has been a criticism that the implementation of smart cities has been too 'top-down'. It has focused too much on efficiency gains and optimisation - new tech for new tech's sake - rather than focusing on the needs of real people. Citizens are seen more as passive sensors rather than active participants who are able to contribute and shape the creation of new city infrastructures.⁴ As data becomes more and more central to our economies and our everyday lives, these criticisms have taken on a new relevance, though issues around privacy and data governance are also becoming more central to the debate.

For instance, the question of who 'owns' data collected in public spaces is currently one which cities are struggling to resolve. In Toronto, the city has come under fire for its decision to commission a sister company of Google - Sidewalk Labs - to build a smart neighbourhood. After two public meetings between Sidewalk Labs and local residents, the question of who will have access to personal data collected, and specifically how it will be used, still remains unanswered.⁵

This section provides a broad overview of why city-based policymakers should care about these issues. While they may not appear as pressing issues to many local policymakers today, it is highly likely that these problems will become more prominent as the use of data and technologies becomes an ever more pervasive part of public life.





1. The smart city agenda is putting individual privacy under threat

Cities want to be 'smart', connected, and data-driven, but in doing this many are unwittingly engaging in large-scale surveillance of citizens. Without greater transparency or accountability around these operations, cities risk a collapse in public trust.

The nature of privacy in urban spaces is being re-defined. It's now impossible for anyone to walk through a large city without data about them or their activity being collected in some way. Cities are becoming 'living laboratories' where networked ICT (wi-fi connected sensors, cameras, reactive lighting, and so on) and digitally enabled infrastructure create continuous flows of data that are used to optimise services.⁶

Growing trends include the widespread and increasing deployment of CCTV and video surveillance in cities. Prominent recent examples include the hundreds of cameras installed by IBM for crime monitoring in Rio for the 2016 Olympics.⁷

In Singapore, Internet of Things sensors and cameras are being placed all over the city to build a '3D map' of the city, to be used for anything from urban planning to measuring crowd dispersion.⁸

Relatedly, predictive policing is growing in popularity for police departments as the availability and volume of citizen data increases. Recent revelations have shown how companies such as Palantir perform large-scale processing of personal data (including of those not suspected of any crime), scraping data from social media, camera feeds, hospitals, parking lots, universities and other private data on behalf of city governments.⁹



City governments have been slow to realise that these technologies are able to create new imbalances of power in our societies. While data has the potential to deliver significant gains, it also gives public institutions – and the technology companies who help install smart city infrastructure – access to vast quantities of highly detailed behavioural data about local residents. As academic Rob Kitchin puts it: people are now *“subject to much greater levels of intensified scrutiny and modes of surveillance ... than ever before, with smart city technologies providing deeply personal pictures of individual lives, especially when datasets are combined together”*.¹⁰

One of the biggest criticisms has been a lack of clear accountability for these decisions. Public-private partnerships have been at the core of smart cities, yet these deals – including the question of who ‘controls’ the data – are rarely subject to any public oversight or scrutiny.¹¹ This has been termed *“surveillance policymaking by procurement,”* a term used to describe the way US cities like Oakland and San Diego acquired and deployed controversial technologies such as facial recognition without elected officials being properly consulted beforehand.¹²

Many companies and local authorities claim that everything they are doing is above board, since they use statistical techniques to anonymise any identifiable information. This provides compliance with data protection legislation, but it has been demonstrated multiple times that anonymisation techniques are not watertight. In one example, anonymised data about the use of taxis released by the New York Taxi and Limousine Commission was used to show where visitors of a local strip bar live, and how frequent their visits were.¹³

As more data is collected in public spaces, it is also becoming easier for machine learning techniques to make connections, and in turn, re-identify individuals within an anonymous dataset.¹⁴ One research paper led by an academic at Imperial College London

proved that a person could be uniquely identified within a large-scale mobile phone dataset of 1.5 million people using only four geolocation data points.¹⁵

It is reasonable to think that the behaviour of most city governments reflects a wider complacency that exists in our society about how personal data is being collected and used. Most people’s behaviour suggests that the public are relatively happy to hand over personal data in return for access to useful digital services, and major concern about these issues is usually only confined to activist or privacy groups.

Yet public opinion surveys often reveal a rather more complex picture. A recent UK poll commissioned by Nesta found that three-quarters are concerned about the privacy of their personal data on the internet;¹⁶ a finding reflected in broader European surveys too.¹⁷ To compound this problem, there is also evidence of a major knowledge gap of how data is circulated and used in the online economy. In a recent UK-based survey conducted by Doteveryone, only a third of respondents are aware that data they have not actively chosen to share has been collected by online companies, and a quarter have no idea how internet firms make their money.¹⁸

Within the context of a broad lack of awareness among citizens, governments have a much more active role to act pre-emptively and as digital safeguards. At a basic level, this requires a role for city governments to educate the public to become as savvy about data as they now are about issues like plastic pollution, air quality or fair trade foods, rather than passively accepting any terms and conditions they are confronted with. A further challenge will be to build legitimacy and greater trust for new technologies in cities, not least finding ways to embed transparency, public dialogue and accountability into how and why data about people is being collected and processed.



2. People have little say over how personal data gets collected and used

Governments also wish to benefit from data sourced directly from citizens (for instance, collected by smartphone apps), but there are few options that allow policymakers to acquire personal data in a more consent-driven way.

City governments realise that a lot of valuable information is collected beyond their administrative boundaries from activities in the wider digital economy. As digital tools and services become more and more pervasive in our daily lives, it is difficult for local authorities to get a full picture of urban mobility, tourism, and finance without access to data collected by external companies.

It has become common for cities to go directly to companies to access the valuable information they collect about local people. Strava, for instance, charges \$0.80 for local authorities to access mobility data on each user.¹⁹ Local governments also enter reciprocal data sharing agreements with app developers, so if a company uses the city’s infrastructure then it should, at the very least, share data back with the city to be used to improve public services.²⁰ Map application Waze trades its own mobility data with local authorities in exchange for real-time data about local construction across the city.²¹ These relationships have become an important part of many cities’ data analytics strategies.

But cities can go even further to create new direct relationships with individuals themselves. As already discussed, many smart cities have been heavily criticised for the absence of effort to integrate citizen voices into how technology solutions are designed and implemented. Google’s aforementioned partnership with Toronto Waterfront to build an entire neighbourhood ‘from the Internet up’ raises questions about whether people will need to sign terms and conditions just to walk down the street. The ability to ‘opt-out’ of processing in public spaces has not yet been fully addressed by smart cities, and it will not be enough to assume that large companies like Google have already done enough to acquire each person’s consent.²²

There are some emerging alternatives that make citizens more active stakeholders in city data analytics. Activities like ‘citizen sensing’ are being trialled across various cities. These projects vary considerably, from those that see citizen sensing as a cheap and potentially more accurate method of collecting data directly from local residents,²³ to those that argue it can empower people with new insights, enabling local government to respond more directly to citizen needs.²⁴

Other trends include new models of social organisation like data trusts, or data co-ops, which offer promising modes of governance that allow people to collect personal data and benefit more directly from it, either as individuals or in groups. Meanwhile, a range of new technologies aim to give people tools to control and share data in more privacy-preserving ways. New trends such as distributed computing technologies aim to build new foundations for data sharing on the internet, embedding transparency and user-control over who has access to data and for what purpose.

In Europe, new legal standards have been set that suggest that this is a moment of opportunity for these alternatives. The introduction in May 2018 of tighter regulations in the form of the General Data Protection Regulation (GDPR) - the EU’s ambitious new data protection law - should pave the way to a future in which people have more control over personal data, including rights to access, erasure and portability, as well as enabling individuals to realise more of the value of data.

With these trends, local policymakers need fresh ideas about how new tools can be supported or implemented that help people to realise their rights, and find innovative use-cases that give citizens more direct control over their digital identities.

3: A misconception about the full value of data

The current digital economy encourages data to be collected and used in ways that create stark new imbalances of power. As a result, cities will need to play a more active role in leveraging more responsible innovation with data in the local economy. This also requires a shift in mindset to see data not as a commodity to be sold, but more as a common good.

The current online economy has enabled digital businesses, through the accumulation of vast databases of personal and behavioural data, to become much more powerful than regulators anticipated.²⁵ As Tim Berners-Lee, founder of the World Wide Web argued earlier this year, the web is now susceptible to being ‘weaponised’.²⁶ One week later, *The Guardian* newspaper revealed that a UK-based firm Cambridge Analytica gained access to the Facebook data of 87 million users, building intimate psychometric profiles that were used to influence the outcome of the 2016 US election.²⁷

The consolidation of power in the internet economy is creating imbalances of power between those who control personal data and those that do not, and increasingly local governments are being required to step in. Last year Uber’s license to operate in London was rescinded, partly due to ‘Greyball’ - a method the company uses to track people, mining personal details from credit cards to target local regulators and prevent them from accessing the service.²⁸ This is not the only story involving this company’s misuse of personal data. After a nine-month ethnographic study of Uber drivers, US-based researchers Alex Rosenblat and Luke Stark concluded that Uber uses collected employee data to leverage significant indirect control - deploying certain ‘psychological tricks’²⁹ - to incentivise desired patterns of work.³⁰ The fact that workers are unable to access or control their own behavioural data reinforces these power asymmetries.³¹

In a recent article, academics Arrieta Ibarra et al., argue that much of the current problem in the data economy can be attributed to the view that data is treated like a new form of money - what they call ‘Data as Capital’. In this view, people’s data is collected and traded by firms; in some cases, it is treated as intellectual property, or only shared for purposes that align with the dominant advertising business model. The problem is reinforced by the fact that data markets are opaque, and long terms and conditions further obfuscate how money is

being made with personal data.³² These authors are among a growing number to suggest that we think about data differently, moving away from ideas of data as a commodity to be bought and sold, and more as a common good that can deliver significant personal and public benefits.³³

If instead of asking what data could be sold by one business to another, we ask what people really need from data, then very different answers come to the fore. Transport has shown some of what can be done. Thanks to open data it is now easy to navigate complex routes, buses, trains or on foot. In the UK, for example, London’s Transport API aggregates transport data from across the city, and now has some 1,500 developers building new services on top of it, fuelling 600 apps and being used by 42 per cent of Londoners.³⁴ Some of the services are still advertising-financed, but the underlying data is treated as common good.

When it comes to more personal data the risks are higher; but so are the opportunities. Data from wearables, connected devices, or other digital trails left behind about our behaviour could drastically benefit society, from mapping pedestrian journeys against pollution, to understanding emerging health issues from the analysis of financial data.³⁵ Yet in the main, the decision about which value is derived from this data is made by the companies that collect it, rather than the individuals who produce it.

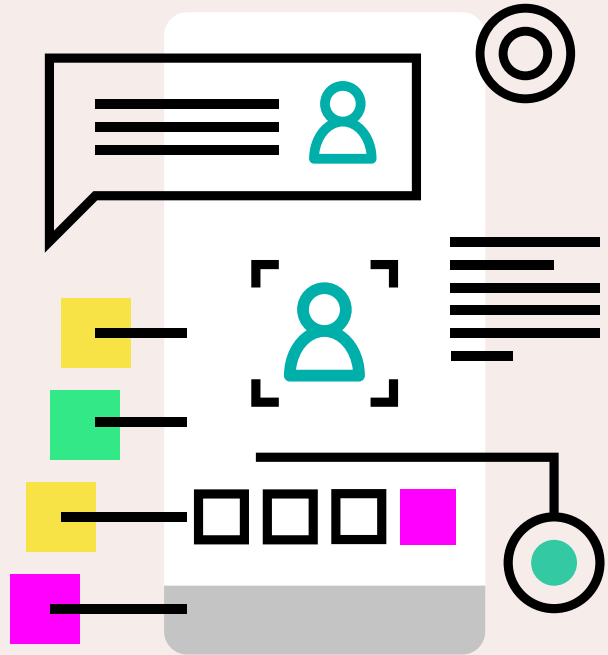
A survey by Nesta in May 2018 found that 73 per cent of people would be willing to share personal data to improve public services, if there was a simple and secure way for them to do so. Inevitably, this will not translate perfectly into action even if clear alternatives are provided. Inertia can prevent people using new tools. But this survey finding demonstrates there is an appetite to create a different type of value from data. To be realised, there needs to be a combination of new tools that are simple and easy to use, capacity building, as well as exploration of new business models for internet firms to decentralise control of data towards citizens.

Governments need to play a role in creating incentives that enable the local economy to deliver more of data's public value, rather than keeping it in organisational silos. Cities such as Barcelona and Amsterdam have responded to this challenge by announcing that data should be seen as a new type of infrastructure. The challenge here parallels that which faced cities in the late 19th century. As the density of cities increased and industrialisation took root, poor living conditions and sanitation problems arose. Cities responded with a series of public works programmes, from sewerage systems, slum clearances and public housing, sanitation works, roads, through to public parks and galleries. These works, funded by the collective to benefit the collective, provided the infrastructure upon which individuals and businesses alike could flourish. The postal service, for example, provided a public good but also guaranteed that individual communications would be private.

Achieving this same goal with personal data will require very different ways of thinking. There are some examples of successful regulation emerging. The UK's recent policy requiring all banks to make personal financial data available with open APIs aims to show that governments can enable individuals to have more portability and control, while creating new incentives that will spur innovation in financial services.

Research has shown that lack of knowledge about the potential for new technologies, both in the public and private sector, is a barrier to realising the value of data.³⁶ This needs to change. Cities face

a challenge to adopt the position of 'custodians' of data. This includes more actively managing the risks that new technologies bring to people living in cities, while ensuring that the benefits of data can be shared equally and in ways that respect individual privacy and prevent new power imbalances from emerging.



A new deal on data

So what practical alternatives are available to cities? In what follows, we explore examples of cities that are pursuing a new deal on data. More specifically we investigate empirical examples of policies and strategies that put privacy and responsible innovation at the forefront of a number of city governments' data strategies. Following the challenges listed above, this report addresses three key policy questions:

1. What are cities doing to build more transparency, accountability and trust in the smart city agenda?
2. What are cities able to do to give individuals more control and empower people to decide how personal data is collected and used?
3. What are cities doing to unlock more of value of data as a common good, while protecting people's privacy and encouraging fair terms of use?



Section 2

Policies for more responsible innovation with data in cities

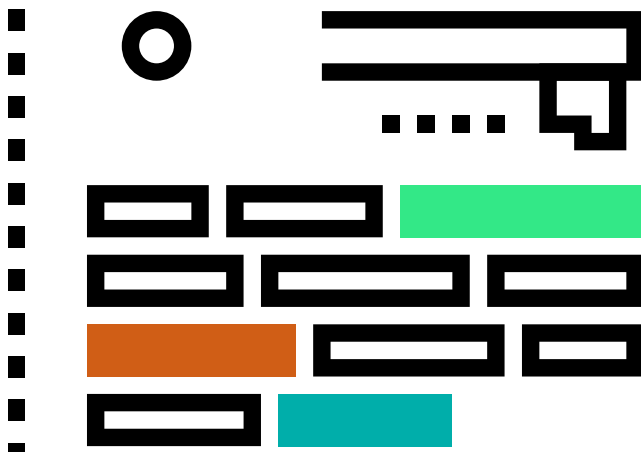
Purpose of this chapter

The last few years have seen an emergence of new projects and policy initiatives by cities to promote and protect people's digital rights. This chapter compiles these programmes and summarises the key policy actions available to local authorities and city governments. It is an overview of what some of the most ambitious cities are doing, and how they are going about doing it.

Research overview

Our aim is to present a vision in which cities can deliver greater privacy and control on the one hand, while also finding ways to facilitate greater sharing of data for social good. This broad view - of more responsible and privacy-aware innovation with data - aligns with the vision of the DECODE project. The aim of DECODE is to provide research and practical tools that focus on how new forms of individual and collective control over data can align with, and help to unlock, data's role as a 'common good.'

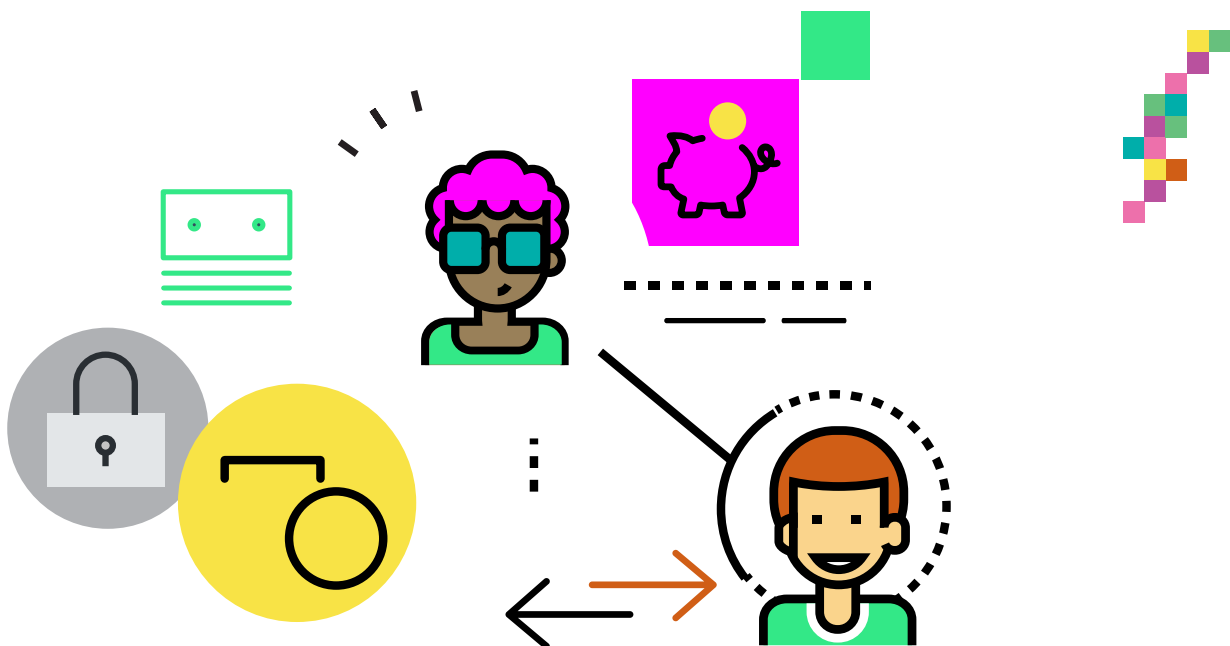
To define common good, this paper builds on previous research of Morell et al., who outline four useful principles for how commons-based models are structured in the digital economy. Although these principles were not designed as policy principles for city governments to follow, they nonetheless provide inspiration for the case studies and summary of policy roles and actions below. As a framework for this report, these principles have been adapted to fit better with the theme of data. They also help us to more clearly define the type of social value which some of the cities below are working towards when they talk about data as a common good.



Fuster Morell et al.'s principles for collaborative commons economy ³⁷	Adapted for specific application to the data economy
<ol style="list-style-type: none"> 1. Peer-to-peer relations, and the involvement of the community of peers in the governance of the platform. 2. Value distribution and governance among the community, whereby profitability is not the main driving force. 3. Developed over privacy-aware public infrastructure, and whereby results favour (generally) open access provision of common resource that favour access, reproducibility and derivativeness. 4. Responsibility to respond to externalities generated by the process. 	<ol style="list-style-type: none"> 1. Governance of data should be democratic and allow clear opportunities for participation over how decisions are made. 2. Data should be portable and easily shared for communal use, whereby profitability is not the main driving force. 3. Data should be available via a privacy-aware infrastructure that allows data to be accessible on consent-driven terms (e.g. tools allowing people to keep personal data private or share for specific purposes). 4. Ensure that there are mechanisms to respond to potential harms caused by data use, including clear accountability.

The five roles of city governments in promoting responsible data innovation

The policies and projects from the case study cities have been translated into a summary of policy roles and actions. This separates policy responses available to city governments into five broad roles. This summary is adapted from the 'policy levers' table developed by Policy Lab, which covers a broader range of activities and spatial levels that were under consideration in this report. We also took inspiration from Nesta's CITIE Index, which is an index created in 2015 to measure how cities around the world are supporting entrepreneurialism and growth.³⁸ The categories are not mutually exclusive and in some cases overlap, but they are still distinct enough to act as a useful guide.



Summary of identified policy roles and actions

Leader

Setting the high-level direction for change.

- Establishing clear guidelines around privacy and responsible use of data.
- Appointing senior leadership and advocacy roles for privacy and data protection in city hall.

Guardian

Making the rules to protect people from harm.

- Codifying basic procedures for identifying and removing risks in open datasets.
- Enforcing transparency over the use of any new surveillance technology.
- Encouraging greater public scrutiny of how data is used to make decisions.

Catalyst

Using procurement and funding to create new incentives for responsible data collection and use.

- Recognising that data is a core added value in public-private partnerships.
- Using ethical digital standards to leverage more responsible innovation with data.
- Creating open protocols to build on.

Provider

Developing new tools and services

- Integrating decentralised data and identity services into local government.
- Piloting state-of-the-art data minimisation and anonymisation techniques.
- Building simple tools that enable easier monitoring and scrutiny of smart city technologies.

Connector

Providing opportunities to participate and building local capacity around a cause.

- Creating consent-driven channels for data-driven participation and data commons.
- Building capacity among local residents to decide how personal data is used.

In what follows we go through each of the policy actions that city governments are implementing under these categories. Although some of the policy initiatives are very recent, we discuss some the challenges facing their implementation where possible. We also provide ‘spotlights’ on more developed examples.



Summary of Case Studies

Barcelona

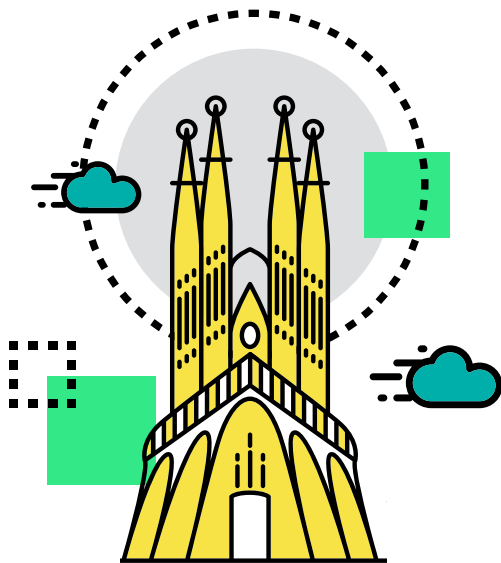
Barcelona has a new digital transformation agenda which conceives of 'data as commons' and attempts to enforce appropriate data privacy protections for citizens. The city has launched a new procurement process designed to incentivise responsible innovation with data and respect for privacy, and

has adopted a focus on open-source technologies. The city government is also providing citizens with practical tools that let them selectively disclose the information they would like to share when using the council's official e-participation tools, while preserving citizen anonymity.

Amsterdam

Amsterdam is home to several projects which promote more responsible use of data across the city. The TADA manifesto, developed by the independent Amsterdam Economic Board, outlines a set of six principles designed to help organisations use citizens' data in a more responsible way. The

Chief Technology Officer's Innovation Team is compiling a registry of all publicly installed sensors across the city. They are also running pilots that will allow people to access local e-government services in an anonymous way, while minimising unnecessary collection of personal data .



New York

New York City is pursuing a range of initiatives which promote the responsible use and handling of citizens' data. One such initiative is the creation of a set of Internet of Things (IoT) Guidelines which establish privacy standards for the deployment of

IoT devices in public spaces throughout the city. The city government has also introduced legislation mandating the creation of a task force to monitor the use of algorithmic decision-making systems by the public sector.

Seattle

Seattle has a comprehensive municipal privacy programme based on a core set of privacy principles and policies. The programme clearly establishes the obligations and requirements of city departments regarding the handling and use of data, and assigns internal roles to support their implementation.

The city's policies mandate the publication of privacy impact assessments and reports about the city's programmes and open data portals, and public engagement on the installation of any new surveillance technologies.

San Francisco

San Francisco has developed an Open Data Release Toolkit to help municipal officials assess the utility and value of publishing a dataset against potential risks to individual privacy. The toolkit

provides leaders with a clear, actionable process for minimising risks, allowing the city to use and release data in a more responsible, privacy-preserving way.

Sydney

Transport for New South Wales, a government agency responsible for public transport in Sydney, has collaborated with Australia's leading data innovation group to apply state of the art differential privacy mechanisms to an open dataset. Differential privacy is a mathematical technique which

minimises the privacy risks associated with the release of open data. In Sydney, the application of differential privacy enabled the release of a two-week data sample from the city's 'tap-on, tap-off' Opal card system for trains, buses, light rail and ferries.

Ghent

As part of their 'City of People' strategy, the Belgian city of Ghent wants to empower its 'smart citizens' by giving them access to 'technology that they own and control'.³⁹ Residents are provided with a simple web-portal called 'Mijn Gent' which gives them access to a range of local services. The city is also

collaborating with a non-profit called Indie on an initiative which will give residents their own personal website, on top of which applications can be built that let them manage and control how local services access and use personal data.

Zug

Zug is providing citizens with a decentralised digital e-identity system. This system issues citizens with a set of credentials, accessed via a digital mobile app, which they can use to verify themselves when

accessing various local services. The e-ID gives citizens more control over their personal data and a more secure alternative to national e-ID projects, such as SwissID, which rely on centralised databases.



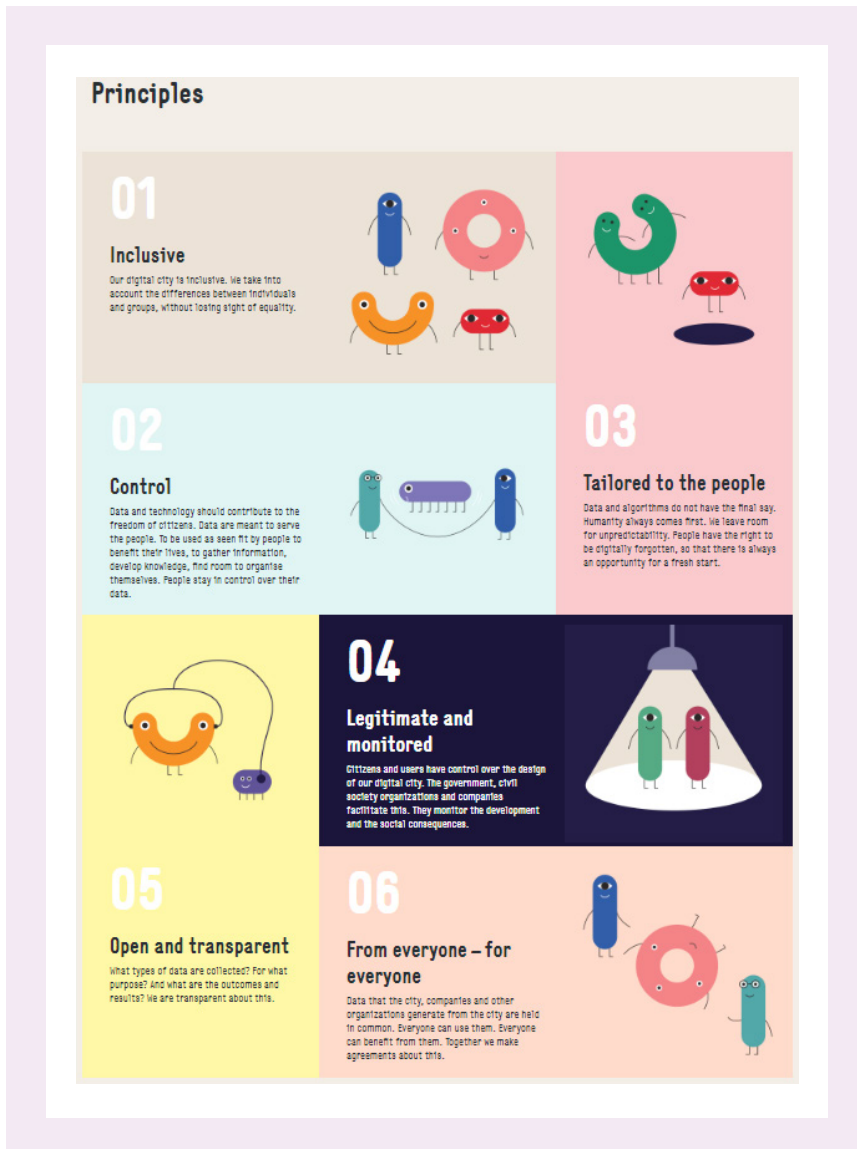


Leader

How is the city setting a clear direction for change, while creating the internal capability to support a more ethical and privacy-preserving smart-city agenda?

Establishing clear guidelines around privacy and responsible use of data

Figure 1: The TADA principles and branding⁴⁰



One of the first steps which many cities take is to make a clear public statement about how the city aims to use data and technology in a responsible and privacy-preserving way. This involves defining a clear set of policies and making them publicly available so that the city staff and service providers can come together around a unified vision.

Amsterdam has shown how high-level policy initiatives can gain broad support from a wide range of stakeholders across the city. For instance, TADA (an anagram of 'data') is a manifesto designed to encourage more responsible use of data in Amsterdam. It was developed by the Amsterdam Economic Board (AEB), an independent organisation which facilitates a network of academic, private sector and government actors. In 2017, the AEB brought together a group of citizens and representatives from government, NGOs and business, and created a set of six principles which companies, cities and other organisations can use to guide their use of personal data.

Smart cities, the manifesto suggests, should be inclusive and tailored to the people (including the right to be 'digitally forgotten'). They should treat data generated by companies as a 'common good', give citizens control over both the use of their personal data and the design of their city, and maintain transparency around their collection and use of data.⁴¹ The AEB's Willem Koeman acknowledges that these principles may be abstract, and therefore the project invested in 'friendly' branding to make the principles visually appealing and easily understandable to the public, as well as actively finding events and conferences to present TADA to raise further awareness.⁴²

The TADA manifesto serves as an example of how an organisation can take a proactive approach towards engaging cross-sectoral stakeholders - including citizens - and spreading awareness around personal data privacy and sovereignty. As of May 2018, the manifesto has 180 signatories from citizens, business leaders, academics and government representatives in the region.⁴³ The council's new coalition has recently committed to implementing the six principles of the TADA manifesto, though there are no details about how this will happen.⁴⁴ The TADA manifesto is deliberately broad, and lacks details about how the guidelines will be properly implemented. The purpose of the exercise has been more about raising awareness and building momentum for new initiatives to develop.

Another ambitious strategy includes the City of Barcelona's Digital City Roadmap: Towards Technological Sovereignty, which was passed in 2016. Barcelona goes beyond issuing a set of broad principles to releasing three policy directives based on putting citizens first, establishing the use of agile methods for ICT projects and proposing a focus on technological sovereignty. This means taking back control of data and information generated by digital technologies, and promoting public digital infrastructures based on free and open-source software, open standards and open formats. It is rolled out in line with an ethical data strategy, where privacy, transparency, collective rights to data and other citizens' fundamental rights are core values.

Detailed implementation manuals derived by the standards were created to guide the work of public officials that implement them. For instance the 'Technological Sovereignty Guide' is a free software management guide that defines protocols, licencing, interoperability, open formats and standards.⁴⁵ The ethical standards have also been translated into three languages and made available on Git repositories, so that other cities can access them, clone the repository and adapt them to their local context. The aim is to create a shared ethical framework among cities for their technology policies, which can become the basis to collaborate on pan-European and global digital city projects.

Figure 2: Barcelona ethical digital standards⁴⁶

ETHICAL DIGITAL STANDARDS: A POLICY TOOLKIT FOR CITIES

<p>Services standard A set of criteria for the creation and management of digital services for the general public, in an agile, open way.</p> <p>Download PDF</p>	<p>Code of practice A set of directives for implementing technological projects using open standards and ethical data management.</p> <p>Download PDF</p>	<p>Agile method Principles and practices for the agile transformation of Barcelona City Council in terms of technology and innovation.</p> <p>Download PDF</p>
<p>Technological sovereignty The practical implementation of technological sovereignty for participants and interested parties in Barcelona City.</p>	<p>ICT purchasing Directives for defining the new model in relation to technology suppliers, based on the Code of Technological Practices.</p>	<p>Innovative purchasing A basic tool for obtaining solutions that are much more tailored to the real needs of sectors and for helping companies to be more competitive.</p>

<https://github.com/AjuntamentdeBarcelona>

- Every city can clone the repository and adapt the guide for itself.
- Git repositories are currently on GitHub platform
- Anyone could contribute doing pull requests, that can be accepted or rejected
- From these AsciiDoc sources, it will be possible to generate stylized visualisations in html and pdf.
- Multilingual (en, es, ca)

AjuntamentdeBarcelona / free-software-guidelines-bcn-en

35 commits | 1 branch | 0 releases | 1 contributor

Clone or download

Spotlight on Seattle: Enforcing a holistic approach to privacy across local government

In 2013, Seattle’s Police Department faced a public backlash over their implementation of a wireless sensor network throughout the city. The network was designed to provide emergency services with their own communication network, but many were concerned that the sensors, which were attached to utility poles, could be used to surveil citizens by geo-tracking their wireless devices.⁴⁷

Controversy also erupted over the Police Department’s use of aerial drones, which were grounded after local residents voiced privacy concerns.⁴⁸ In the aftermath of these incidents, Seattle implemented a comprehensive municipal privacy programme, and is now considered to be a city leader in the field of data privacy.⁴⁹

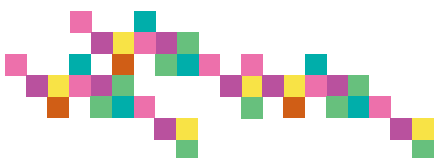
Seattle’s privacy programme was developed in 2015 and relied heavily on knowledge from different internal departments as well as external expertise across the city. It convened a group of representatives from across all 15 government departments, while also inviting a Privacy Advisory Committee made up of thought leaders in academia, local companies, lawyers and community activists to feed in further recommendations.⁵⁰ Six ethical guidelines were subsequently outlined that broadly define how Seattle should collect, use, store and share personal data, and affirm the city’s commitment to maintaining accurate information and valuing citizens’ privacy.⁵¹

Seattle’s Privacy Programme also includes an Open Data Policy,⁵² which was developed in collaboration with various partners, including the University of Washington. This policy stipulates that government data should be ‘open by preference’, meaning that the city reserves the right to withhold data if it has the potential to cause privacy harms.⁵³ Under the

policy, datasets must be reviewed for potential privacy harms prior to release, and an annual risk assessment must be performed of both the Open Data Program and Open Data Portal.⁵⁴ The Open Data Policy was introduced by a Mayoral Executive Order,⁵⁵ which directs all city departments to adhere to the policy.

In 2017, Seattle also issued an Ordinance which outlines a range of procedures designed to increase transparency around the city’s use of surveillance technologies. This includes the creation of an inventory of all surveillance technologies and the preparation of Surveillance Impact Reports for new technology.⁵⁶ Examples of technology under review include Automated License Plate Recorders, which are attached to police vehicles, and Emergency Scene Cameras.⁵⁷ That said, the Ordinance has also been criticised for broad exemptions to its definition of what counts as a surveillance technology, including policy body cameras and various sources of video surveillance.⁵⁸

A range of municipal officials are assigned specific roles to manage the implementation of the Privacy Programme. For example, Chief Privacy Officer, Ginger Armbruster, is responsible for providing ‘overall leadership and direction’, while Open Data Champions manage their department’s publication of open data.⁵⁹ Seattle’s approach illustrates how foundational ethical principles about the management and collection of personal data can be translated into tangible, enforceable policies and practices across a city. The first annual risk assessment conducted by the Future of Privacy Forum identified Seattle as ‘a national leader in privacy program management’, and scored the City a five out of six in the areas of ‘Data Quality’ and ‘Transparency and Public Engagement’.⁶⁰

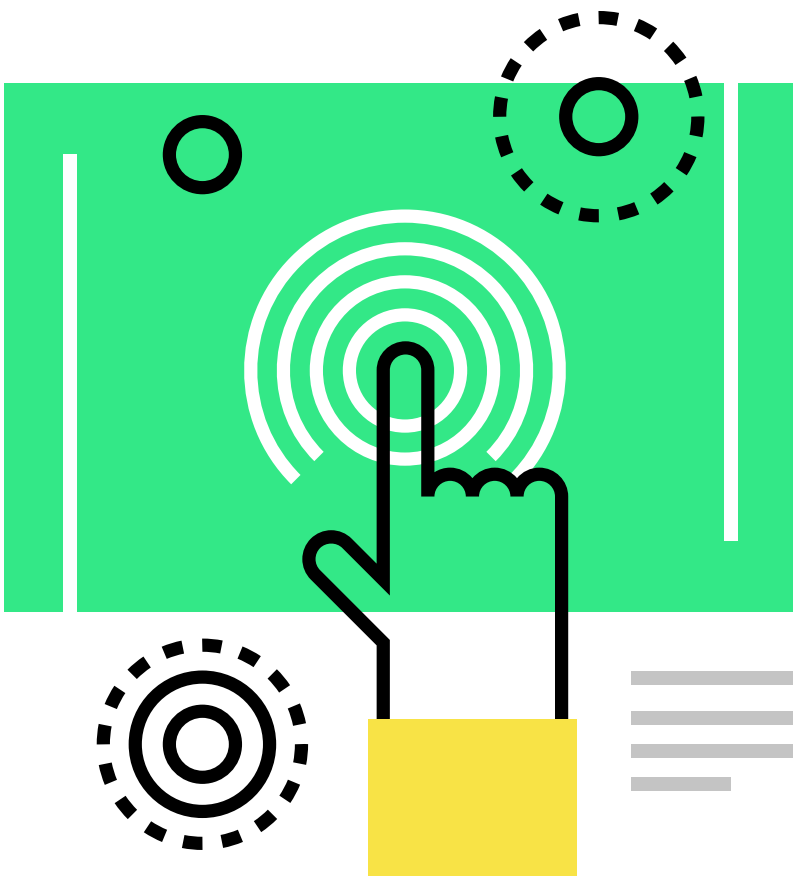


Appointing senior leadership and advocacy roles for privacy and data protection in city hall

City governments are embedding principles of responsible data use more concretely by assigning clear internal responsibilities for these issues. One option is to hire dedicated roles to implement procedures that codify ethical data management across city government. Creating these roles across the council helps establish a clear commitment to the issue. What's more, by appointing senior leadership roles cities can build a much greater level of accountability around the use of citizens' data.

In Europe, Amsterdam's 2018 coalition policy manifesto includes a commitment to create an 'information commissioner' who will work with a municipal privacy officer to ensure commitment to 'privacy by design principles'.⁶¹ In the US, the appointment of Chief Privacy Officers is an increasing trend. Santa Clara County appointed a CPO at the end of 2017, whilst New York is one of the most recent US cities to have made the announcement.⁶² The Officer will have a duty to create policies and protocols on information sharing throughout government, while requiring that each agency issue clear guidance on privacy practices to each of its employees and contractors.⁶³

In Seattle, the Chief Privacy Officer role provides 'overall leadership and direction to the Privacy Program', including working with the City Auditor to assess compliance with the city's Privacy Principles. The city's Privacy Program also created a number of other roles to embed good privacy practices across the council. This includes departmental 'Privacy Champions' across different agencies to handle basic enquiries, conduct and sign-off low-risk privacy reviews, and escalate or reporting issues to the Privacy Program Manager, who is responsible for coordinating the Privacy Champions and 'cultivating a community of practice to share knowledge and best practices'.⁶⁴



Guardian

How does the city create rules to protect people from potential harm caused by digital tools, and ensure that the use of data-driven technologies is able to benefit everyone?

Codifying basic procedures for identifying and removing risks in open datasets

Councils have increasing access to data collected from new data points across the city, on anything from environmental pollution to mobility. It has become common to publish much of this information as open data. But as technology becomes more sophisticated and the amount of personal data collected across the digital economy grows, the potential to re-identify individuals in an open dataset is increasing. Some councils are therefore making efforts to create simple tools that guide staff through the benefits and risks of publishing open data. Codifying basic walk-throughs and simple toolkits can be a useful way to ensure that best-practice is easy to follow for staff across different departments.

San Francisco launched an open data platform called DataSF in 2009, with the aim of using data to improve city services. Recognising that current privacy laws do not always prevent re-identification through anonymised data, the government released an Open Data Release Toolkit in 2016, which is designed to guide municipal officials through a risk assessment process prior to the publication of open data.

The toolkit provides a framework which helps municipal officials assess the utility and value of publishing a dataset against potential risks to individual privacy.⁶⁵ Using a four-step model, it helps officials identify sensitive datasets, perform risk assessments and select privacy solutions such as data aggregation, k-anonymisation, and geo-masking. In some instances, it will recommend that a dataset remain closed. Notably, the toolkit is not used for public record datasets, and does not address privacy concerns relating to data collection or storage.⁶⁶

Already, the city San Francisco Public Library has used the toolkit to revise how they release data about the public's use of the library, limiting the specificity of geographical boundaries in the dataset to reduce the risk of re-identification.⁶⁷ In other instances, the toolkit may actually enable the release of data that would otherwise remain closed, thus enabling researchers to access information that could be harnessed for social benefit. This was the case for the San Francisco Mayor's Office of Housing and Community Development, who used the toolkit to release previously unpublished data about citizen engagement with affordable housing projects.⁶⁸

In addition to simple walk-throughs, other cities like Seattle have privacy specific training – 'Data Camp' – for city staff who have responsibility over publishing administrative open data. The Data Camps are multi-day workshops designed to educate staff about issues like data quality, data privacy, data equity and public disclosure. Even non-technical employees receive the training.⁶⁹ According to the Future Privacy Forum, who independently reviewed Seattle's Open Data Program, this kind of training ensures that 'data are more likely to be protected throughout their lifecycle (collection, use, release, disposal)'.⁷⁰

Enforcing transparency over the use of any new surveillance technology

Seattle’s implementation of a ‘wireless sensor network’; Oakland’s creation of a ‘data integration center’ bringing together all its surveillance infrastructure; and San Diego’s deployment of facial recognition technology, are examples of decisions that were made about controversial smart city technologies with little public oversight.⁷¹ In many cities, the decisions around which technologies are adopted or used by local government lie with executives within city departments. This means that the provision of private technologies can be approved with only partial awareness that these negotiations have taken place by elected council officials, let alone members of the public.

Concerns have been raised by citizens and privacy campaign groups about the installation of these technologies. It has led a number of US-based cities to enforce greater transparency over the installation of such technologies. Dubbed the ‘privacy localism’ movement, these cities have been aided by the work of the American Civil Liberties Union (ACLU). ACLU’s ‘Community Control Over Police Surveillance’ campaign provided a series of model policy recommendations to help local governments better oversee and regulate the use of police surveillance technologies.⁷²

Santa Clara County in Northern California was one of the first US local authorities to act on these recommendations, requiring county agencies to provide a detailed report on how new and current surveillance technologies are being used to investigate crimes, as well as requiring those technologies to pass public scrutiny at an open meeting prior to use.⁷³ In 2017, New York City Council also introduced a bill called the Public Oversight of Police Technology (POST) Act, which aims to increase transparency around the New York Police Department’s (NYPD) use of surveillance tools by mandating the publication of ‘surveillance impact and use policy reports.’⁷⁴ These reports include basic information about the capabilities of surveillance technologies, rules and processes around their use and ‘any safeguards and security measures designed to protect the information collected.’⁷⁵

Seattle’s approach is also notable for its strong emphasis on public engagement. The city government’s Surveillance Ordinance, passed in 2017, requires all city departments to review and list all existing surveillance technologies, which the regulation defines as technologies designed to ‘observe or analyze the movements, behaviour, or actions of identifiable individuals in a manner that is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice.’⁷⁶ For any technology that meets this criteria, the relevant government department must complete a Surveillance Impact Report (SIR). Each stage of report is updated alongside each item on a publicly accessible tool that lists all of the surveillance technologies managed by the city. Prior to the council approving a surveillance technology, the relevant department must host public meetings and invite feedback on the technology via a web tool.⁷⁷

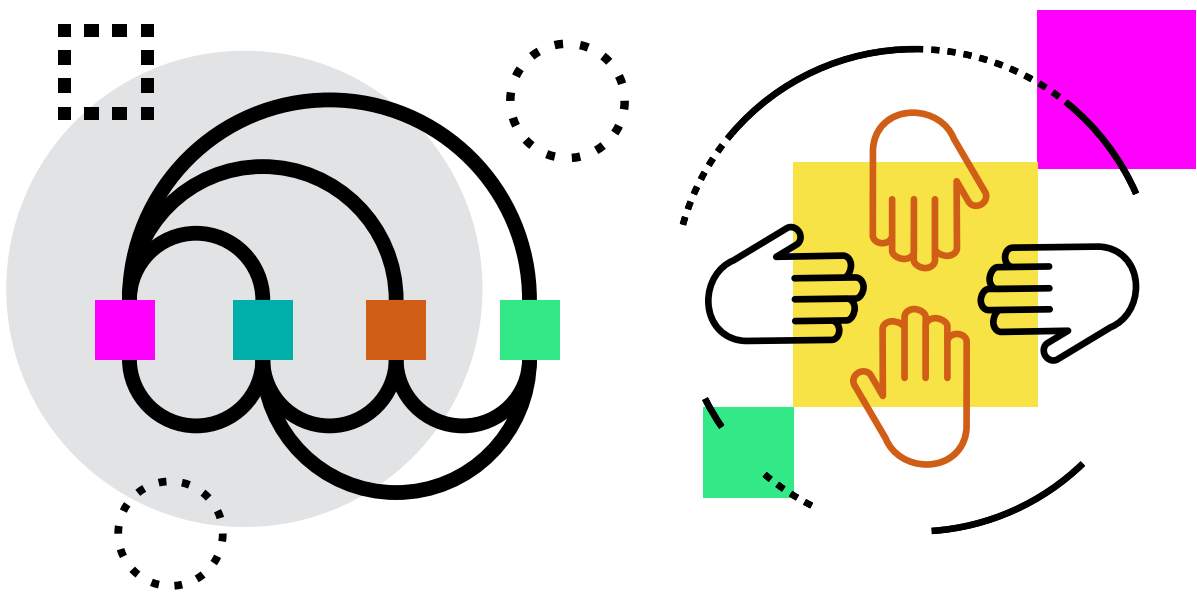
More recently the city of Oakland has raised the standard further, extending the definition of surveillance technology to include any software used for surveillance-based analysis. It also demands higher levels of transparency, prohibiting non-disclosure agreements with technology vendors.⁷⁸ In the past, non-disclosure agreements have been used by manufacturers to explicitly prevent local authorities from sharing basic information about the types of equipment being contracted, how they are being used and how much the technology costs.⁷⁹

Encouraging greater public scrutiny of how data is used to make decisions

How cities exploit the data they collect has recently become a central topic of concern in the smart city movement. Sometimes there are very specific types of harm that can be caused when data is aggregated, analysed and used to make decisions. For instance, the increasing use of algorithms across the public and private sector refers to the use of historic data points to make predictions about future behaviours. These predictions can then be used to make decisions about how an organisation deals with an individual or group, and can have discriminatory and exclusionary impacts.

In cities, the predictive power of this technology is being used in ways that complement or in some cases replace decisions previously made by public officials, from assisting police in targeting crime to determining how much social care support people need.⁶⁰ In practice, some studies have found these to disproportionately target people from certain groups, most notably ethnic minority groups in the case of predictive policing.⁶¹ While other studies have found no evidence for racial bias in predictive policing, this is at the very least an issue that city officials and technology companies should be aware of. In addition, the algorithms being used to make statistical inferences are often complex and opaque, making them difficult for public administrators, let alone citizens, to understand how decisions are arrived at.

In response, the New York algorithmic accountability task force was the first policy proposal of its kind in terms of a city-based institution with a mandate to inspect the operation of automated decision systems used by local government. Their initial proposals were radical, requiring vendors of algorithmic systems (often including private sector providers) to open all of their source code for public inspection. The strict requirements proposed by the bill were perhaps one of the reasons it struggled to gain widespread support, and was eventually watered down. Nonetheless the initiative has set a precedent worldwide for cities to take bolder steps in the monitoring of automated decision-making systems across the public sector and by private service providers.



Spotlight on: New York's Algorithmic Transparency Bill

In a bold legislative move, New York introduced a law designed to increase transparency around the use of algorithmic decision-making systems in the city. Across the world, algorithms are increasingly used to determine everything from school allocations to eligibility for bank loans.

The proliferation of such systems in both public and private sectors has led to growing concerns about the potential impact of algorithmic bias on citizens' lives. For example, a journalistic investigation by ProPublica found evidence of racial disparities in algorithms which are used by the US criminal justice system to assess defendants' likelihood of re-offending, and thus their eligibility for release.⁸² There is academic work which challenges these findings,⁸³ but it suggests that bias or fear of bias (even if unwarranted), can stymie potentially beneficial schemes.

In 2017, New York City Council member, James Vacca, introduced a bill calling for the establishment of a task force to monitor New York city agencies' use of automated decision-making systems. *"If we're going to be governed by machines and algorithms and data,"* Vacca said, *"they better be transparent"*.⁸⁴ After multiple revisions, the bill was passed through the City Council and became law in January 2018. The task force will be responsible for publishing a report in December 2019, which will outline recommendations about the use of automated decision systems by the city.

More specifically, the task force will recommend procedures which will help the city to identify systems which disproportionately affect particular demographic groups, and address instances where a citizen is harmed by such a system.⁸⁵ This will include procedures which give citizens the right to an explanation of such decisions and the right to contest them.⁸⁶ The task force will also need to develop a procedure for making information about automated decision-making systems public, including technical information where appropriate.⁸⁷ Finally, the report will assess the feasibility of a procedure for archiving these systems and their data.⁸⁸

The task force was announced by Mayor Bill de Blasio in May 2018, and includes officials from city agencies and the administration, representatives from affected citizen groups, and academic experts in the field of automated systems.⁸⁹ It will be co-chaired by Emily Newman, the Acting Director of the

Mayor's Office of Operations, and Brittny Saunders, Deputy Commissioner for Strategic Initiatives at the NYC Commission on Human Rights.⁹⁰ Their recommendations have the potential to spearhead procedures which may create more transparency around the use and impact of algorithmic systems in New York City.

Introducing the bill, however, was not a smooth process for Vacca's team. Initially, they faced a lack of interest and engagement from city officials. As Zachary Hecht, who co-drafted the bill, acknowledges: *"It wasn't an issue that exactly resonated with City Government. It was not something that everybody was thinking about"*. To generate interest, Vacca's team gave officials tangible examples of the impact of algorithmic decision-making systems in the city, and pitched an exclusive to the *New York Times*. As a result, the first Technology Committee Hearing about the bill was one of the most well-attended in recent memory.⁹¹

Yet the bill faced considerable opposition, and the first iteration had to be drastically scaled-back before being passed into law. Originally, the bill called for agencies to openly publish the source code of their automated decision-making systems and allow members of the public to submit data to the systems for self-testing. However, at the Technology Committee Hearing, businesses and policy experts expressed concerns about the open publication of source code, which they felt could compromise businesses' proprietary information and lead to security risks in the public sector.⁹² When re-drafting the bill, Hecht acknowledges that they had to adopt a less ambitious agenda: *"we started to realise that while we felt source code should be public, it wasn't necessarily a precondition for transparency and accountability"*.⁹³

Going forward, the task force will face several challenges. The first will be how to define what legally constitutes an automated decision-making system.⁹⁴ The second is that the city does not currently have an inventory of public sector automated decision-making tools or spending on algorithmic services, which may impede the work of the task force.⁹⁵ Hecht also acknowledges that there are concerns amongst some advocates that the report's recommendations will have limited impact and that the task force may only address the 'low hanging fruit'.⁹⁶

Catalyst

How is the city leveraging its buying power to create new incentives and encourage more responsible innovation in the wider economy?

Recognising that data is a core added value in public-private partnerships

As more and more urban services become data driven, the question of who controls and has access to data brings major political and ethical dilemmas. As Francesca Bria the Chief Technology Officer of Barcelona told us: *“the question of who owns what in the smart city and who is controlling the urban infrastructures physical and intangible is key. The question of who controls and owns data is thus central”*.⁹⁷ As a result, a core part of the city’s new strategy conceives of ‘data as a commons’, akin to a new kind of public infrastructure that is subject to democratic control. This includes management of city data, open data, official statistics and external data collected by third parties within public spaces, or on behalf of the city.⁹⁸

One of the main ways the city is trying to realise this vision is through its renewed procurement strategy. Barcelona has recognised that procurement can be used to encourage more responsible use of technology to protect citizens’ digital rights, strengthen the local economy, and make it more open and sustainable. The council has an annual contracting budget of around €600 million (almost 25 per cent of the municipal budget), which makes it an important driving force for economic activity in the city.⁹⁹

Local government now includes clauses within procurement contracts specifying that a service provider must make any data that may be of public value available to the city council in machine-readable format. The objective is to prevent the development of silos of data, while allowing greater democratic oversight over the data being collected across the city:

“Data is a new meta-utility, a public infrastructure like water, roads and the air we breathe. More and more, data and information is the added value of the service itself, so while you are procuring public services, you need to make sure data remains in the public domain with the right privacy protection, since it belongs to the citizens”.¹⁰⁰

What is more, by incorporating the data using open standards and open APIs, the aim is for data to become a ‘public good’ that can be used to solve city challenges. For example, the council has been negotiating with telecoms company Vodafone for a year to hand over anonymised mobility data about people living in the city. Previously this information remained behind closed doors, but now the council is running a programme in partnership with a local startup accelerator, running challenge prizes that involve small companies, social enterprises and cooperatives, who compete to use the data to find applications that solve local problems. This is done at the same time as preserving high standards of citizen privacy and accountability.

The vision of Barcelona’s Chief Technology Officer is that cities can help to create a European ‘commons data pool’. It will set ethical standards to access and share this data, including terms set by citizens themselves (through projects like DECODE, described in greater detail below), as well as allowing local entrepreneurs and companies to build a new generation of data-driven public services on top, from mobility, to healthcare and hospitality.

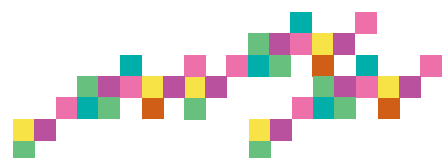
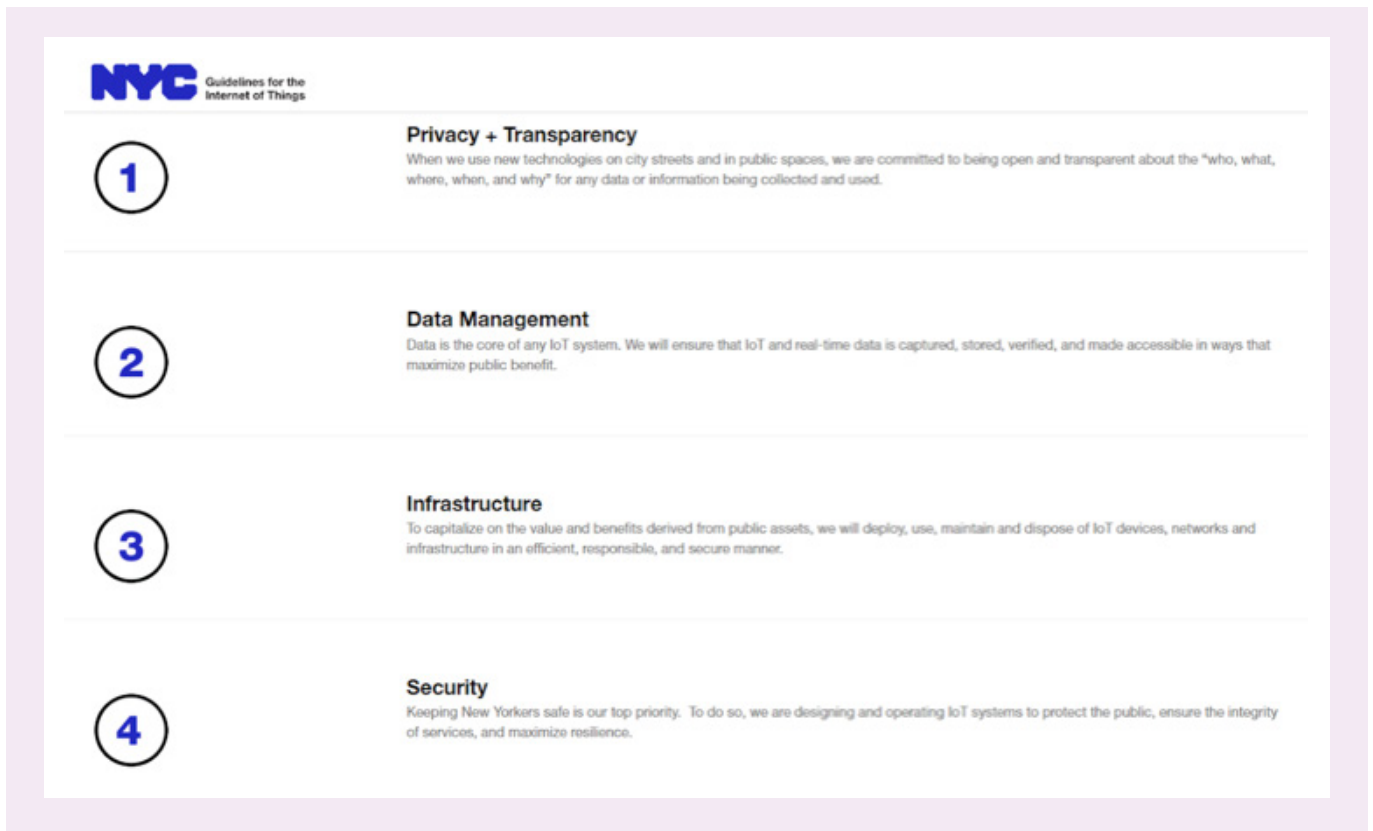
With Barcelona's ambitious procurement plan in place, it is worth mentioning that the council is still in the early stages of transformation. It is clear that, in the short term at least, there may be challenges facing implementation. As Malcolm Bain, a lawyer assisting the council on its digital transformation strategy, describes: *"the trouble with these policy measures is they're all on paper and then people don't fully respect them. You have to actually convince all the people in procurement and project management that they have to actually monitor that. Because you can paste these fantastic clauses in the contract But do we have the time, the money, the processes?"*¹⁰¹ Bain also pointed out that there was lots to be positive about. The council has already advanced its internal training and project management processes, and has issued big contracts including these standards that have been respected by vendors.¹⁰²

Using ethical digital standards to leverage responsible innovation with data

Councils have also begun to use their buying power to request that specific design principles are embedded into technologies they use.

New York's 'Guidelines for the Internet of Things' policy framework, was released by the Mayor's Office of Technology and Innovation in 2016. The Guidelines were developed to assert privacy standards around the deployment of IoT devices which use city assets or are installed in public spaces.¹⁰³ For example, they assert that IoT devices should only collect data for 'explicit and legitimate' purposes, all personally identifiable information should be anonymised, and that city agencies should keep an inventory of IoT devices.¹⁰⁴

Figure 3: New York's 'Guidelines for the Internet of Things'¹⁰⁵





The IoT Guidelines are designed to encourage consistent practices across city agencies when procuring new technology products in the city, and to help municipal officials understand and mitigate the risks associated with IoT deployments, and provide transparency to both the private sector and general public about the city's policies.¹⁰⁶ In a pilot project, the New York Parks Department applied the framework when installing a 'smart' park bench. Use of the framework led to a range of actions, including a Privacy Policy created jointly by the Parks Department and technology vendor describing the process by which data from people's phones are captured for data analysis, being immediately anonymised and used only for the intended purpose of counting the number of people using the park. It also included a new data ownership and management agreement with the smart bench vendor, identifying who owns the data being collected, the data management responsibilities and instructions for accessing open APIs that can be used to extract data from the vendor's platform.¹⁰⁷

However, while the Mayor's Office of Technology and Innovation oversees the 'broad enforcement' of the IoT guidelines, they do not hold the same status as laws, and thus it may prove challenging to monitor compliance.¹⁰⁸ As one academic commentator put it, the guidelines "*may be nothing more than recommendations*".¹⁰⁹

Creating open protocols to build on

Many of the cities that are putting responsible use of data in their smart city strategies make a conscious effort to promote the use of open-source technologies. This is driven by the ethical argument that publicly funded technologies delivering a public good should be transparent and open to public scrutiny.

But using open-source also makes collaboration easier. A problem for smart cities is that technology vendors often build proprietary data solutions, which lack interoperability and can become technological 'silos' that make the council reliant on private technology providers. By only using open-source components and standards, city governments can encourage interoperability between different software projects across the council.¹¹⁰ Again, Barcelona is a prominent example. Its use of open-source means that the council is able to require that sensor manufacturers and other companies provide their data in standard format. This is not necessarily about privacy or data protection, but it is about creating incentives so that more city data can be made available for public benefit.

**Spotlight on:
Barcelona's open-source technology stack**

Barcelona has built a clear vision for how different open-source technical components will fit together to enable the safe collection and sharing of data for public benefit.

Barcelona's 'Sentilo' was built to operate as the city's main sensor platform, receiving real-time data from Internet of Things sensors all across Barcelona.¹¹¹ This also maintains transparency for sensor operations across the city, as Jordi Cirera, Sentilo Project Lead, told us: *"we knew we would have thousands of sensors deployed in the city ... So we knew we needed a catalogue of what we have[,] ... all sheep go through the same door."*¹¹²

Currently Sentilo only acts as a platform for 'factual' data, that is, information about the environment, air quality, noise, and so on. But Barcelona now has more ambitious plans to integrate citizen-sensed data into Sentilo. This would open the city's official sensor platform to citizens (i.e. not just technology companies and the council), while also allowing people and communities to share data more easily with the city.

While Sentilo acts as a collector of real-time sensor data, 'CityOS' acts as the city government's internal data lake - a single access-window for all datasets

across the council. The city's Chief Data Officer looks after CityOS and decides who can access what. Some of the datasets are made publicly available under different degrees of openness via APIs. Currently the platform is entering the final stages of production and a range of new datasets are being added, some of which will be available via publicly accessible tools, such as via Decidim, the city's official digital democracy portal, and a user-friendly data dashboard called BCNow. We elaborate on how citizens will be able to interact with these tools in the 'Connector' section below.

More broadly, the council is undergoing a general transition to freedom technologies. Seventy per cent of investment in new software development is today free and open-source. This eliminates many overheads in terms of software licences, and the freedom to choose providers also helps to increase the reinvestment of public money to boost local tech entrepreneurship. It also aims to prevent vendor lock-in and reduce long-term dependence on a small number of tech firms. The policy has been coupled with the creation of a digital marketplace for small-scale providers, to assist Barcelona's growing technology sector of around 13,000 companies.



Provider

How is the city adopting new tools and services that respect each person’s right to privacy and promote greater individual control over personal data?

Integrating decentralised data storage and identity services into local government

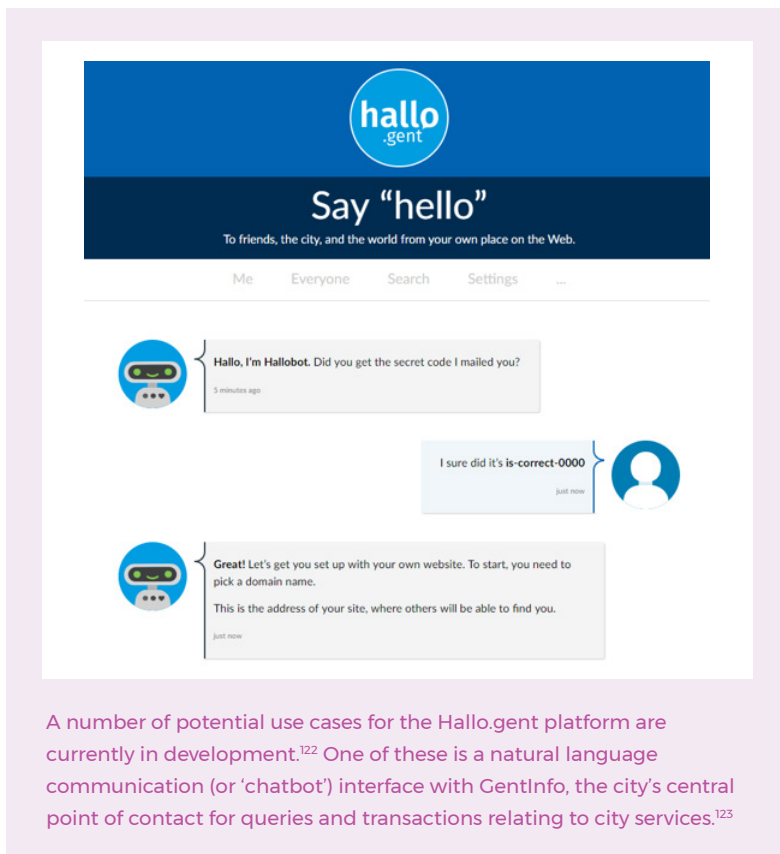
Opting-out of public services provided by the state is often not an option; people rely on these services and may have no other choice but to use them. This places an important responsibility on city governments to be proactive in rolling out services that provide good data protection and privacy by design. In our research we found that many cities and local governments are becoming test-beds for new technologies that give people more control over personal data and their digital identities.

City officials reported that the prevalence of so many local services in cities makes them ripe for experimentation with new types of privacy-preserving digital services. According to Ghent’s Chief Strategy Officer, Karl-Filip Coenegrachts, “We have over 250 local applications at the local level alone that have additional information on local residents on top of the national register”. This includes a range of services from registering for sports camps and shelters for homeless, as well as simpler transactions like registering complaints.¹¹³

As part of Ghent’s ‘City of People’ strategy, the government wants to create a city of ‘smart citizens’ who are empowered ‘with technology that they own and control’.¹¹⁴ One of the city’s projects to achieve this has been the provision of an online data profile called ‘Mijn Gent’ (‘My Ghent’), which contains a more detailed, enriched local version of Belgium’s national personal data registry.¹¹⁵ The online profile allows citizens to access government resources, such as library services or registration for sports camps, while giving them full control over the management and sharing of personal data.¹¹⁶ For example, if a citizen registers for a local event with their children, they can choose whether they share information about the number of people in their family.¹¹⁷

Building on the My Ghent profile, the city has been collaborating with Indie on an initiative called ‘Hallo.gent’, which aims to give Ghent citizens their own online domain and ‘federated personal website’ (e.g. ‘JanJansen.gent’).¹¹⁸ Coenegrachts describes it as like giving people their own ‘piece’ of the internet, like a social media profile where data and the domain itself is controlled and owned entirely by the individual citizen.¹¹⁹ The aim is for Hallo.gent is to create user-friendly applications on top of the My Gent data profiles, that are “as convenient and enjoyable to use as Facebook or Twitter”.¹²⁰ The system will allow the citizens to register for local services, and the council can verify different pieces of information from residents available on their own My Ghent portal, without the council ever needing to collect or store any additional personal information.

Figure 3: Hallo.gent Prototype¹²¹



A number of potential use cases for the Hallo.gent platform are currently in development.¹²² One of these is a natural language communication (or ‘chatbot’) interface with GentInfo, the city’s central point of contact for queries and transactions relating to city services.¹²³

Spotlight on Zug: Decentralising identity verification for local government services

In order to streamline Switzerland’s administrative and business processes, the Swiss government has made the development of an electronic identity (e-ID) a national priority.¹²⁴

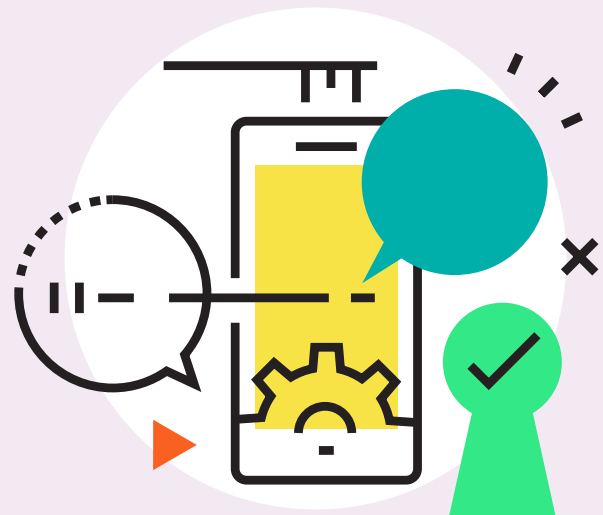
However, the Federal Council is outsourcing the development and implementation of the e-ID technology, and the current national ‘SwissID’ initiative is a joint venture between private corporations and banks such as Credit Suisse and UBS. The Mayor of a small Swiss city called Zug, Dolfi Mueller, argues that the provision of an e-ID by private firms using centralised computer databases erodes citizens’ trust: *“You have to trust the ID provider. ... Use of new technologies like blockchain could make this feeling of trust stronger”*.¹²⁵

In response, the Swiss city of Zug partnered with the Lucerne School of Business and Zurich tech firm ti&m to roll-out technology which enables Zug residents to register a digital e-identity on the Ethereum blockchain. The system does not require reliance on any private co-operation to operate, and enables a much higher degree of accountability and individual control over who has access to personal data.

Zug’s blockchain-based e-ID lets people authenticate themselves on digital services simply by revealing a credential which is signed by the city council, and encrypted and stored on the user’s own private device. The decentralised alternative not only helps to build trust between citizens and government, but also minimises the infrastructure requirements for the city, which can avoid the burden of hosting a large server or database.¹²⁶ Use of the e-ID also gives citizens more control over the disclosure of their personal data, and for service providers, facilitates compliance with GDPR, as only minimal information is exchanged between parties.¹²⁷

To create their digital identity, Zug residents must first download the uPort mobile app, which was developed by Ethereum tech company ConsenSys. After registering on the app and the Zug ID web portal, citizens must verify their identity in-person using official government documents. Once verified, they can use their encrypted uPort-ID to engage with e-government services such as online voting and bill payments, access proof of residency documents and issue e-Signatures.¹²⁸ The first e-ID was issued on November 15, 2017, and by February 2018, approximately 220 Zug residents had registered.¹²⁹

While Switzerland’s previous attempts to roll out a national e-ID have failed, the potential expansion of the national, corporate-backed SwissID may threaten the future of Zug’s small blockchain project. As Mueller acknowledges, *“[SwissID] can exert much more pressure on people to have such a digital ID. They are Goliath, and we are David”*.¹³⁰ The resilience of Zug’s e-ID project will, in part, depend on the success of its use-case pilots and uptake with the local community.



Piloting state-of-the-art data minimisation and anonymisation techniques

People are constantly asked to give out personal information about themselves in order to use online services. Airbnb, for instance, requires an ID verification like a passport or driver's license to check that hosts on the platform are authentic, whereas a whole range of other services frequently ask for basic information from phone numbers to postcodes and email addresses. Alongside the decentralised identity solutions mentioned above, a number of technologies are emerging which help to minimise the amount of personal data that needs to be collected when providing people with a service. Where the risks of identification remain high, new technical tools can also help to anonymise, separate or obfuscate data, providing additional protection to citizens. Cities (often through partnerships with research institutions) are playing an important role as testing grounds for these techniques.

The European Commission-funded DECODE project is currently developing technology in Barcelona and Amsterdam that will allow the council to verify certain aspects of local residents' identities in an anonymous way. The technique being applied, known as 'Attribute Based Credentials' (ABCs), lets citizens choose to reveal selected 'attributes' about themselves rather than their full identities when interacting with council services. These could instead be simple pieces of information such as 'this person is over the age of 18' or 'this person is a resident of the city of Amsterdam'.

In Amsterdam, landlords who wish to let their property through platforms such as Airbnb are only permitted to do so for a maximum of 60 days per year, and must list their property on an online holiday rental registry with the council.¹³¹ Therefore the first DECODE pilot in the city will enable accommodation providers to register their properties with the municipal government in a privacy-preserving way. Using a set of simple attributes, landlords will be able to register their holiday rentals with the council whilst sharing only essential information about their property and number of days rented. The only people who will be able to identify a person will be the council's enforcement team if they visit a local resident's address and ask for their ID.

This creates a system whereby the council collects the minimum amount of personal data possible. Aik van Eemeren from Amsterdam's Chief Technology Office highlights the need for more secure local government services: *"We collect too much information now, but there is no other way. It's a technical solution to enable data minimalism on this. It's not there yet, and we need it"*.¹³² If successful, the cities will gain confidence and experience with technology that has in-built privacy by design.

That said, beyond simple authentication procedures there are still many examples of data collection by city governments where risks of identification remain high. Data about public transportation services is often collected without people knowing, yet it can provide valuable information to researchers and municipal officials tasked with improving city services. Like other forms of open data, such information can compromise citizens' privacy if travel patterns are de-anonymised.¹³³ Indeed both the availability and variety of data, alongside modern machine learning techniques, make it increasingly possible to reverse-engineer anonymised datasets.

To mitigate the risks of re-identification, in March 2017, Transport for New South Wales (TfNSW)¹³⁴ collaborated with Australia's largest data and innovation group, Data61,¹³⁵ to release open data about citizens' use of Sydney's public transport network using a technique called differential privacy. Differential privacy is considered the 'gold standard' of anonymisation techniques. It is not necessarily a tool or technology, but rather a 'formal mathematical definition'¹³⁶ which improves privacy, often by adding random 'noise' to data.¹³⁷

The open data that was released was a two-week sample derived from Sydney's 'tap-on, tap-off' Opal card system for public trains, buses, light rail and ferries. Recorded in July and August 2016, the data was made freely downloadable and included information about trip dates and the time and location of 'tap-ons' and 'tap-offs'.¹³⁸

New South Wales has an ‘open by default’ data policy, which favours the release of government data unless it is against the public interest (e.g. if the data exposes personal information).¹³⁹ In this instance, the application of differential privacy allowed for the data to be released for public benefit whilst preserving citizens’ privacy. One basic analysis conducted by a researcher from the University of Technology Sydney highlighted how the data could be used to help businesses plan their opening hours and staffing arrangements around peak travel times at public transport stations.¹⁴⁰ Deputy Secretary Braxton-Smith also suggested that the data “could also help local councils, government authorities and service providers to better plan local works and services provision in the neighbourhood”.¹⁴¹



In an academic review of the pilot, researchers found that, ‘in some unusual circumstances’, there is a very small probability that an attacker could detect the ‘presence’ of a small group or individual, but not any identifiable information.¹⁴² As a result, the Opal dataset ‘does not technically meet the precise definition of strong Differential Privacy’, but this could be ‘easily corrected’ in future.¹⁴³ Notably, the researchers used this finding to encourage openness about data privacy mechanisms, which they suggest is ‘crucial for engineering good privacy protections’ and ‘might help improve the privacy of future releases.’^{144, iii}

Spotlight on: Privacy by design and smart city technologies

‘Privacy by design’ is an approach that attempts to minimise risks by requiring that privacy and security considerations are built into the design of any technology from the very beginning of its inception, rather than being bolted on at the end. A variant of privacy by design – ‘Data protection by design’ - is now a legal obligation for data controllers as part of the new General Data Protection Regulation. However, for many years privacy by design principles have come under dispute for being overly vague and open to interpretation.

Nonetheless, there are some other examples that show what these principles might look like when applied in practice in the case of smart city technologies. For instance, the city of Zwolle in the Netherlands has a privacy and security-enhancing architecture underpinning its smart grid project, which includes 250 participating households. The project used a privacy by design process to secure sensitive data, which includes detailed information about household energy usage and preferences for smart appliances. To create the privacy-enhancing infrastructure, mechanisms were put in place to

minimise, separate, aggregate and hide sensitive data. For example, data is aggregated to a residential area, consumer choices about smart appliances are separated from the electricity supplier, and no personal data is processed by the distribution system operator.¹⁴⁵

In the US, Chicago’s ‘Array of Things’ project aims to create an open, modular network of sensors designed to collect real-time data on the city’s environment. The project has an oversight board and a privacy policy, but many of the protections for citizens are embedded into the design of the network itself. The project relies on technological instruments to ‘specifically avoid any potential collection of data about individuals’, and privacy protection ‘is built into the design of the sensors’.¹⁴⁶ For instance, the sound sensors only collect data on ambient volume without recording or transmitting raw microphone data, and all images being processed by cameras will be processed into numerical data after which image data will be immediately deleted.¹⁴⁷

iii. One drawback of privacy-preserving mechanisms is that they can often reduce the utility of a dataset. In this instance, the application of differential privacy means that researchers cannot analyse users’ trips and journeys, because their ‘tap-ons’ and ‘tap-offs’ are not linked. Therefore, practitioners that wish to use differential privacy will need to assess the balance the anticipated benefits available from the data with the cost and effort required with applying these techniques.

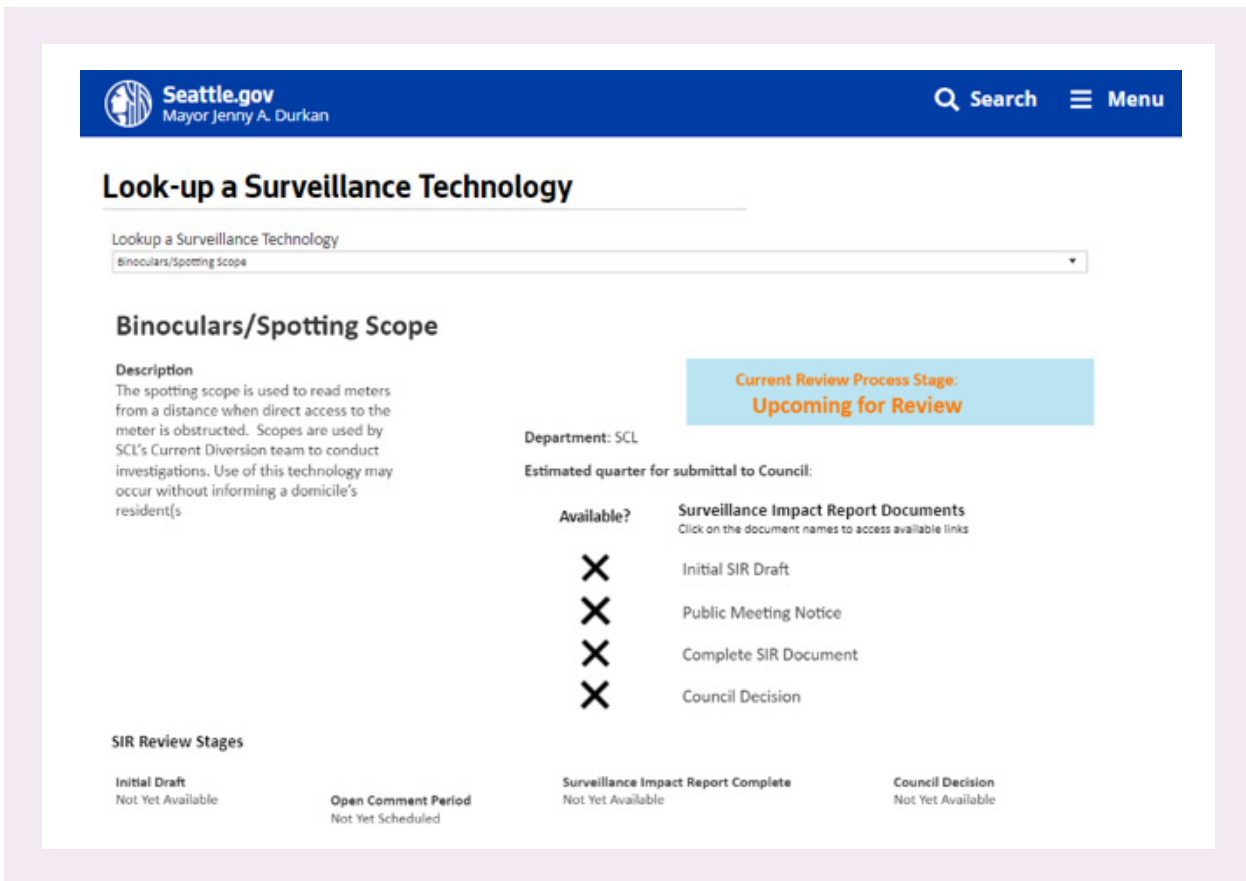


Building simple tools that enable easier monitoring and scrutiny of smart city technologies

The collection and use of personal data from sensors, including cameras, microphones, motion and wi-fi tracking sensors, has the potential to identify individuals and cause harm if used improperly. Therefore, in order to build trust with residents, the city has a responsibility to keep track of the location of sensors, and the purpose of data collection. A small number of city governments are making concerted efforts to publish this information openly so that installation of sensors can be subject to sufficient public scrutiny.

Some cities have begun to compile publicly accessible lists of sensors located in public spaces. Seattle, for instance, has a 'Look up a Surveillance Technology' tool on its website which compiles examples from across different city departments.¹⁴⁸ Encouraging the private sector to submit information about their sensors is a much bigger challenge.

Figure 4: Seattle's 'Look up a Surveillance Technology' Tool¹⁴⁹

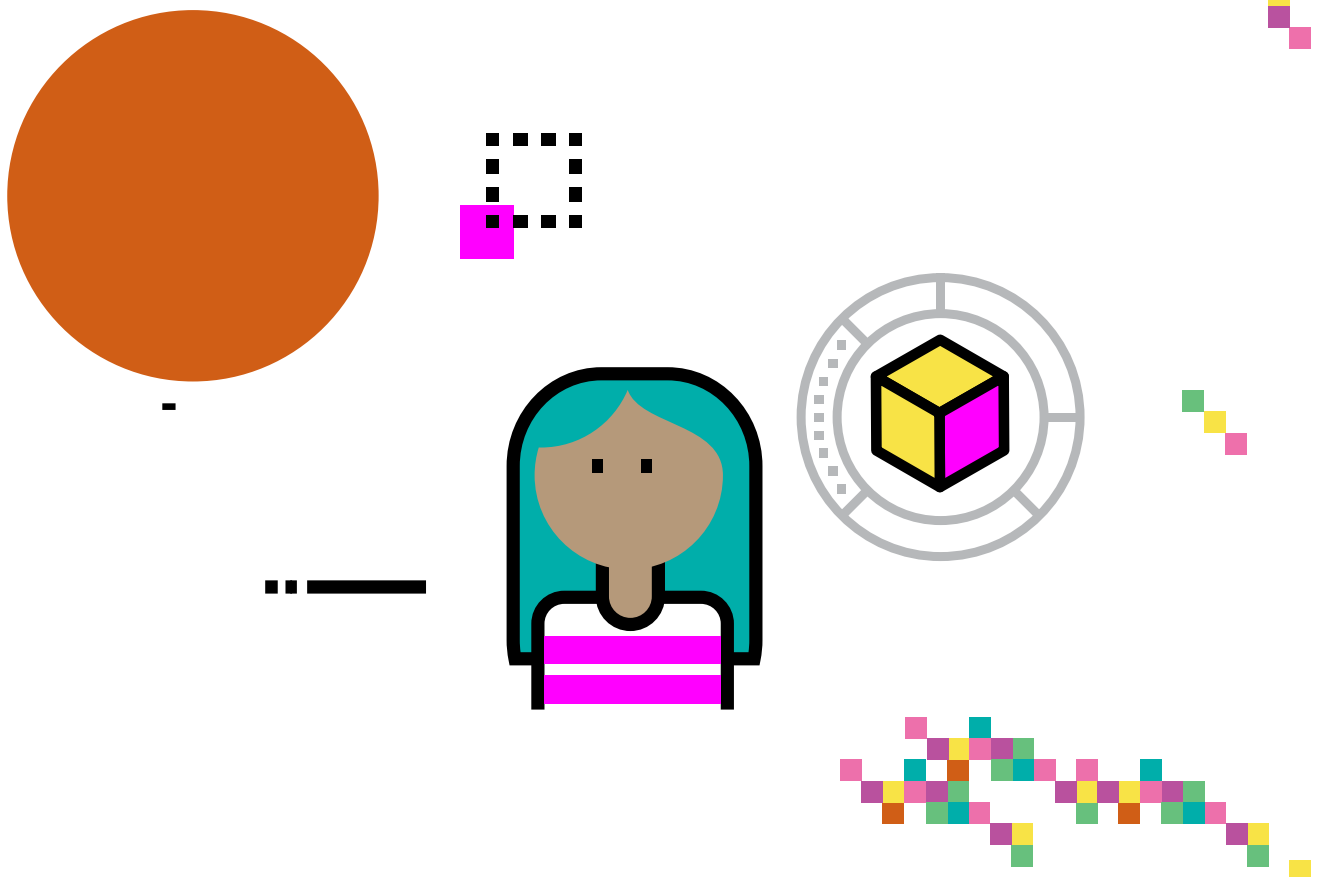


In Amsterdam, the Chief Technology Office is working with a consortium of local businesses to build a 'sensor register' for all sensors installed across the city by both local government and the private sector. The aim of the project is to provide a single repository, including information about the type of IoT devices and their location, as well as the type of data they collect. This will make it easier for citizens and civil society groups to keep track of where sensors are,

while providing guidance on how to make complaint if a person or group is unhappy about the location or purpose of data collection (say, if a sensor is located uncomfortably close to someone’s house). Entrepreneurs will also be able to access this information and request permission to use the data by contacting the owner (who remains anonymous), and citizens will be able to file objections about particular sensors with the municipality.¹⁵⁰ By June 2018, the Council aims to have a proof of concept, and will test the feasibility of the registry over the following two years.¹⁵¹

The successful implementation of the sensor register project requires accurate and comprehensive data on the location of sensors in the city. Accessing this data will be a key challenge for the city council, as companies may be reluctant - or unable - to reveal information about the location of their sensors and the type of data they collect. Theo Veltman from Amsterdam’s Chief Technology Office says: *“We have several indications that most companies don’t know where the sensors are - because they’re scattered around companies. One department has a couple, the other has a couple, and so on”*.¹⁵² Indeed, Veltman also acknowledges that the possible reluctance of companies to reveal information to competitors may limit the success of the register.¹⁵³

Mandating transparency around sensor location will be difficult to enforce, meaning that the project will begin on a voluntary basis. This limitation suggests that, in addition to building new tools that encourage greater transparency, further action may be required by the council to properly encourage more responsible data collection practices in the wider economy. Veltman argues that the process of enforcing these requirements will be an ongoing challenge for the council, and *“more difficult than most people think”*.¹⁵⁴ In future, registration on the sensor inventory may become a planning requirement for organisations wishing to install a public sensor in the city. Registering sensors may also be a requirement for companies who wish to tender with the council.



Connector

How does the city collect and use personal data in a way that fosters high quality and consent-driven engagement with citizens?

Creating consent-driven channels for data-driven participation and data commons

Data provided by citizens themselves can be a valuable source of information for local authorities, helping them to develop services around what matters most to residents. Many governments already benefit from citizen-sensed data in various ways, usually by negotiating with smartphone app providers. In recent years, a range of examples have shown how accessing data directly from citizens can provide access to fine-grained, and more accurate data about what is happening across a city.

Notable examples include those like the Japanese city of Date which distributed sensors to children under the age of 16 and pregnant women to measure radiation in the aftermath of the Fukushima disaster. Analysis of the individual dosimeter data from the city found that actual radiation exposure was four times less than the levels recorded by the government helicopter sensors.¹⁵⁵ Local government in Christchurch, New Zealand has run a project called Sensibel that provides cyclists with a bluetooth-enabled 'bell-like' device that can be attached to the handlebars of a bike. Cyclists can click the device to record positive and negative experiences throughout their journeys, and then 'annotate' their journey map with text and photos using the Sensibel App.¹⁵⁶ The city has also experimented with helping citizens with chronic obstructive pulmonary disease by equipping them with 'smart inhalers' to detect high-risk locations.¹⁵⁷

These examples demonstrate that city governments can gain access to more useful and indeed more personal data when there is more active and conscious contribution from the people involved. This highlights a potential tension for future citizen-sensing projects. While many of these projects demonstrate the value that new types of citizen-sensed data can bring to local policymaking, few have found ways to introduce proper consent mechanisms for this kind of processing. This is likely to become more of a challenge as sensors become more ubiquitous and personal data becomes more intimate. Indeed smart cities have often struggled with the notion of 'aggregate consent', and how they can gain consent from large groups of people when collecting personal data in public spaces.

DECODE is one project which tries to create tools that give people the power to withdraw or dynamically control the nature of their consent on an ongoing basis. Barcelona City Council - the project's lead co-ordinator - will use the tools to give citizens simple ways to share data on their own terms.

The city's Chief Technology Officer, Francesca Bria, describes how this goes well beyond the conventional vision of open data, where information is simply made available and can be freely shared with few restrictions or rules of use: *"For instance, I want to share my transport data with the city to do 'X', but I don't want to share it with another third party. And these are then the citizen set rules that should be enforced when data consumers access the data ... It's about how you set the policies that allow the city to put this data in the public domain."*¹⁵⁸

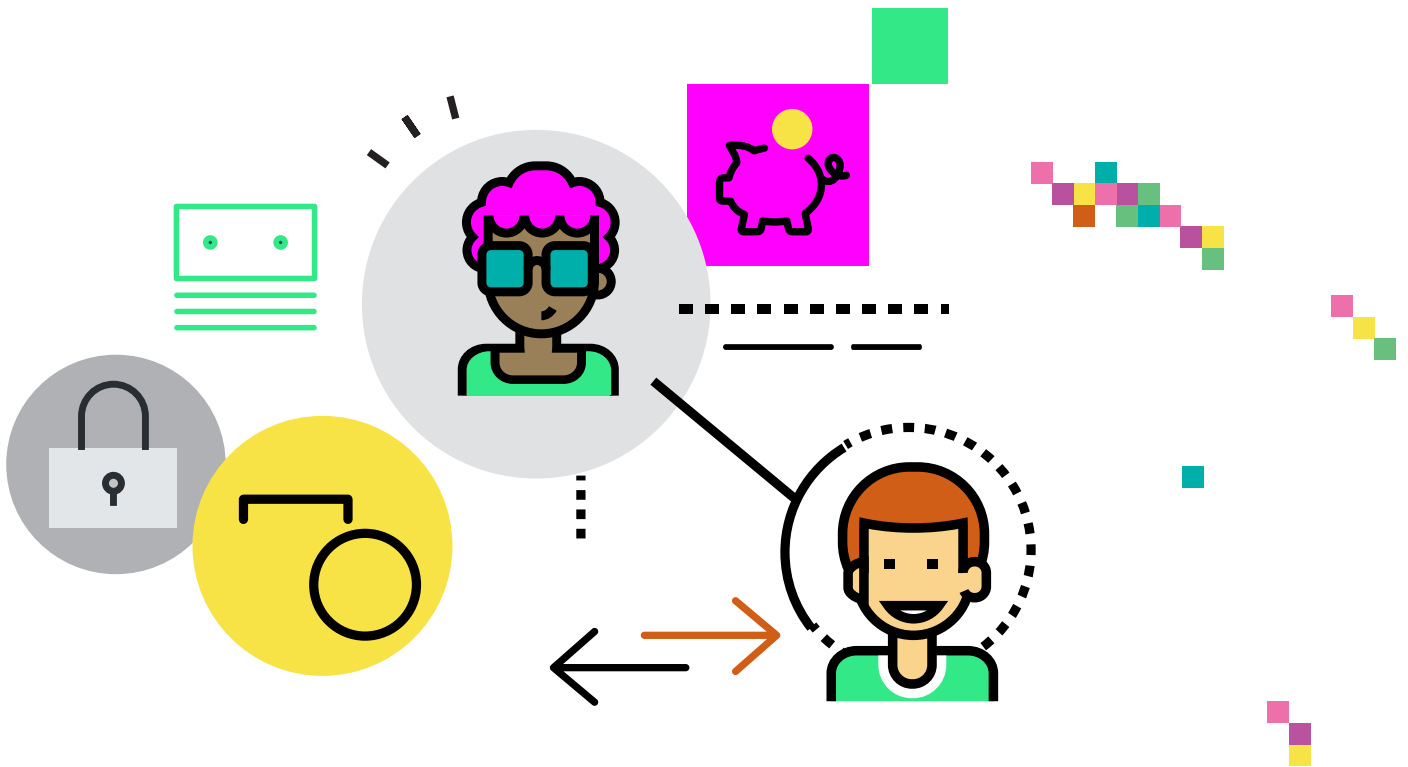
DECODE technology will be integrated into council services, allowing citizens to set specific 'entitlements' to personal data, such as who may access the data and for what purpose. *"The entitlements will be linked to data commons licenses and made enforceable by using DECODE smart contracts as well as Attribute Based Credentials (ABC) to encode rules about who can have access to specific data, and use encryption to ensure only authorised parties get access."* explains Francesca Bria.¹⁵⁹

For example, the city government will be piloting this technology using Barcelona’s official e-participation platform, Decidim. Citizens can use the platform to propose ideas, run surveys, take part in the city’s annual participatory budgeting process, or participate in consultations organised by local councillors. The basic premise for the first DECODE pilot is that digital democratic participation and a healthy public sphere require effective privacy protections. Currently the platform has around 30,000 active users, but many in the Decidim community have expressed concern that sharing their views on the platform will expose their political affiliations to the council, or to future administrations.¹⁶⁰ Therefore the pilot will allow users to sign petitions and engage in debates anonymously - while still authenticating residents - using the DECODE application mentioned above. They will also be able to set specific permissions over how personal data is shared (regarding age, gender and location).

Another DECODE pilot will create simple tools that allow people to collect data from within their neighbourhoods about noise and environmental pollution (also see the next section), as well as providing a data commons dashboard and privacy-enhancing recommendation system named BCN Now, with a visualisation tool for citizens, allowing citizen-sensed data to be displayed and blended with a range of other information sources - including administrative open data, and other personal information.¹⁶¹ These will be developed in ways that provide strong privacy and anonymisation protections, and control for users when they collect and share data. For instance, from these dashboards, citizens will set permissions about who has access to their data, for how long and for what purpose using DECODE integrated functionality.¹⁶²

Figure 5: BC NOW dashboard¹⁶³





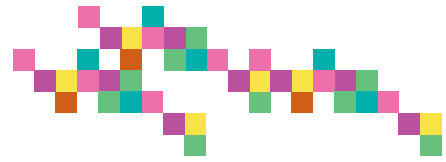
In the past it has been a challenge to persuade council staff about the benefits of data that is collected by the citizens themselves. Initially the council was highly sceptical about the reliability of the data. It took several tests to persuade the council that the citizen-owned sensors' reliability was accurate and worthy of their attention. According to Bria this culture within the council is now changing with the new city's plans: *"we are going from the previous kind of [more dismissive] approach to empowering citizens and understanding the value of their data."* The council is now linking smart citizens' sensors to the city sensor platform Sentilo, and opening Sentilo to citizens as a result. The city is also exploring what it means to jointly create policies and actions from the bottom-up with the citizens, and is taking a more open minded approach to learn from, and respond more effectively, to what citizens are doing.¹⁶⁴

Building capacity among local residents to decide how personal data is used

Providing digital tools is an important step for governments to take, but without supporting efforts to build awareness and capacity in the population there is a risk people will not adopt them. There are multiple examples of this in the recent past, from digital participation exercises, which attract no participation, through to open data portals, which are never being used. Simply building something is no guarantee people will either want to use it or know how to.

In many cases the technical tools that allow citizen-sensing to happen are just one part of a much broader outreach strategy to identify the issues that matter to people and then to build local capacity so that they can use the tools and be empowered to make a difference in their community.

For instance, 'The Bristol Approach to Citizen Sensing', developed in partnership with a think-tank based in Barcelona called Ideas for Change, is a strategy that the UK city has adopted to place people at the heart of innovation in its smart city strategy. The method uses inexpensive open-source sensors (called The Smart Citizen Kit) to change the way environmental data is collected, empowering citizens to take more control over their local environment. The method is committed to making sure its work is inclusive, and runs workshops and training programmes to upskill local residents.



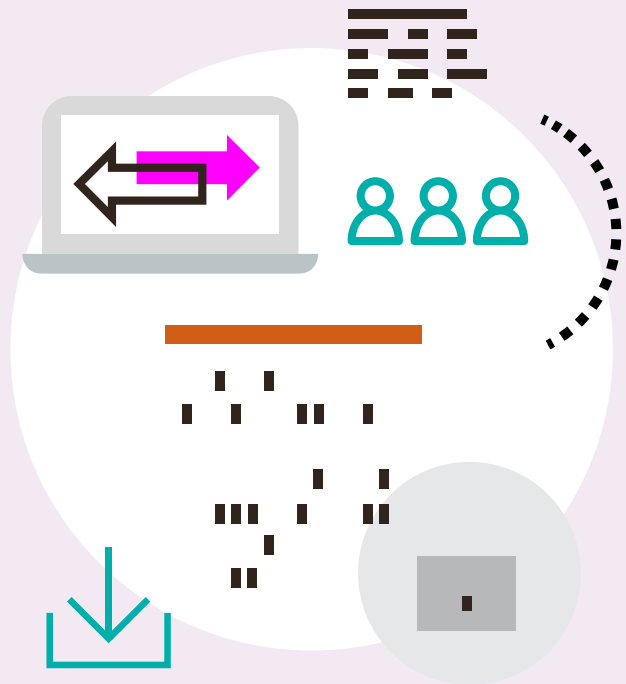
**Spotlight on:
The Bristol Approach to citizen-sensing**

In 2015 Ideas for Change worked with Bristol City Council and Knowle West Media Centre (KWMC) to develop a participatory citizen-sensing pilot in Bristol. It involved three months identifying ‘hotspot conversations’ with local residents, and local groups who might be interested to take part.

This was followed by another three months framing the issues, inviting community groups with an interest in the issues to meet one another, and clearly define problems that affected them. This included identifying problems facing local people - in this case damp homes was the issue which had the most momentum - while also exploring how technology could help them address it, and demystifying words like ‘data’.¹⁶⁵ As Ideas for Change CEO Mara Balestrini describes:

“The city council and Knowle West Media Centre (KWMC) asked us ‘how do we work with people in data projects in a way that is bottom-up and in a way that is empowering to people?’ ... [T]he first step is identifying the issue ... it turns out that the issue of damp was a big problem, especially when you have a housing crisis - there is no incentive for landlords to take care of the problem, because if you don’t want the house somebody else might even pay more to have the house. So why would they solve it? We saw there was a huge opportunity to demonstrate how you can shift power structures when you bring the data to the surface, and that’s how the whole thing about damp sensing came up.”¹⁶⁶

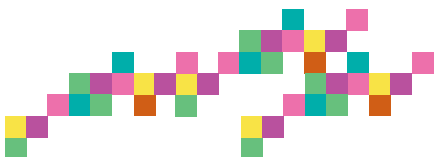
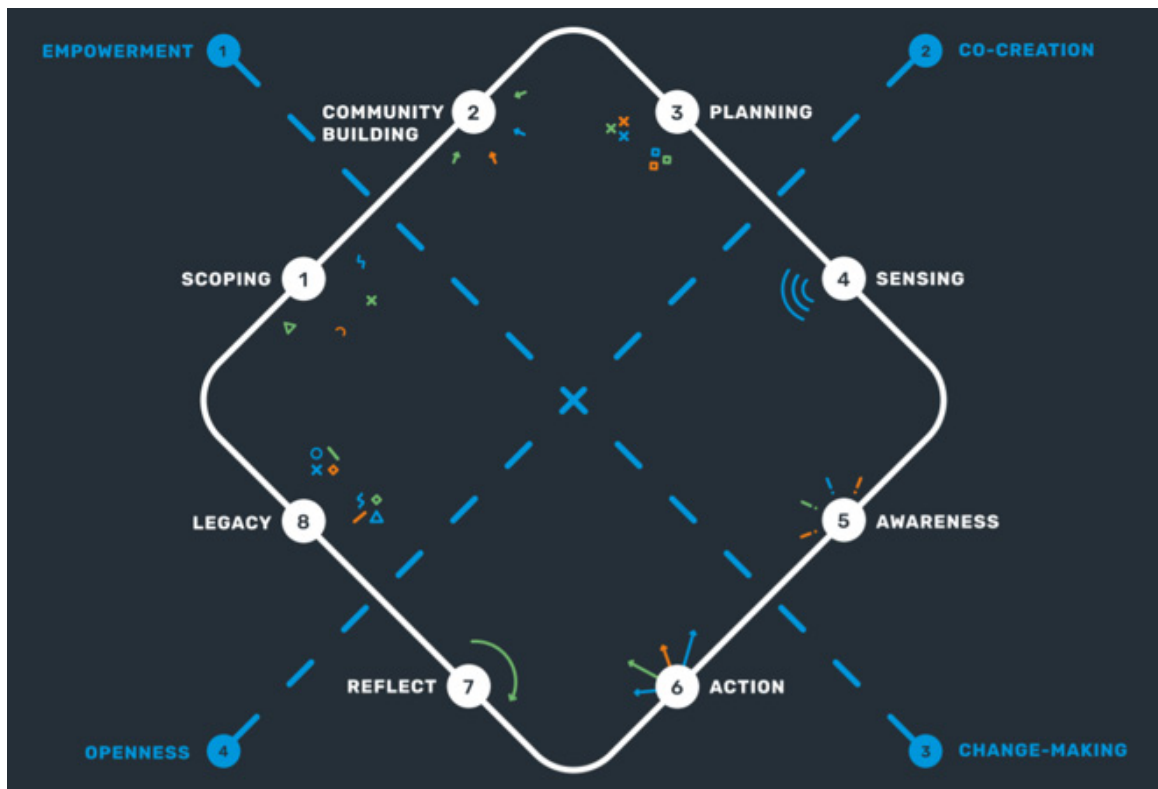
The tools were then designed and deployed in close collaboration with the end-users. Residents were given a sensor to install in their homes, which measured the temperature, humidity and ‘dew point’, and they were asked to keep a diary of events that might lead to damp - for example, when someone is showering, cooking or washing clothes. This information combined with the data from the sensor, helped the council (and residents) to better understand what conditions create damp and how best to respond: it ‘opened up a new layer of data that didn’t exist’.¹⁶⁷ It also helped to bring members of the community together around the issue, as well helping them learn new technical and data literacy skills.¹⁶⁸



In another notable example, Ideas for Change worked with communities in Plaza del Sol, Barcelona, to help them install sensors that measure the harmful effects of noise pollution in their neighbourhood (as part of the EU-funded Making Sense project).¹⁶⁹ The council organised public meetings in which locals could talk through their findings, and propose potential solutions. Some of the solutions that have been implemented include new flower beds that remove areas where people used to sit and drink, more signs and banners requesting people to be quiet, and improved community policing.¹⁷⁰

Like in Bristol, the project shows how it is possible to unlock more of the communal value of the data by bringing people together to decide how it is used. Although technology played an important part as an enabler, success depended heavily on community mobilisation and active outreach by the council. It is therefore a reminder that technology will only play one role within any broad effort to make local politics more participatory and responsive to local people.

Figure 6: Making Sense Toolkit Methodology¹⁷¹





Summary of policy outcomes

The sections above show how a range of city governments are becoming more savvy about how they collect, manage and use data. These are not simply abstract arguments or principles. Enacting these policies can have clear and tangible benefits both to citizens and the council staff. We have summarised five key benefits which are emerging for the city governments that we spoke to below:

City council staff are building confidence in navigating the risks and opportunities of new technologies.

Privacy training programmes like those in Seattle give local staff the skills to understand, and where possible mitigate, risks brought about by new data-intensive technologies. Barcelona's efforts to integrate ethical digital standards into government contracts, and to improve broader technical skills of those in the contracting department are giving staff the confidence to negotiate with technology companies in ways that bring city data into public ownership which, in turn, can be used in the development of new policies or services.

Clear privacy procedures and protections for individuals open up new opportunities for data of public interest to be shared.

It can often be difficult for council staff to find an ethical and proportionate balance between the risks of sharing data versus not sharing. In the case of New South Wales, the application of sophisticated anonymisation techniques allowed for transport data to be released for public benefit whilst preserving citizens' privacy. San Francisco's Open Data Release Toolkit demonstrates how clear and actionable processes for minimising privacy risks can enable data that was previously closed to be shared (including information that is of significant public interest in the case of the council's community housing data).

Cities more easily achieve compliance with data protection legislation (like the GDPR) reducing burden of unnecessary storing and managing of personal data.

Decentralised identity systems like those being piloted by Zug reduce the requirement for costly, centralised data centres; while projects like DECODE allow people to be 'authenticated but anonymous' when accessing a range of council services. Other

smart city projects like Chicago's 'Array of Things' automatically minimise data collection and delete unnecessary information once it has been used. As the regulatory environment becomes tighter, these tools not only protect individuals from privacy harms but also can help to reduce regulatory burdens by embedding legal compliance into the operation of the technology itself.

Use of open-source and open standards improves transparency and leads to less duplication of smart city technology projects, benefiting the council and local entrepreneurs.

The open-source urban platforms being built by city governments, like Barcelona's Sentilo or Amsterdam's sensor register, enable greater awareness of installed sensors and data being collected across the city. They also encourage entrepreneurs to better understand what smart city projects already exist, or even request that other sensor owners share their data. By acting as a clear standards setter, the council encourages interoperability between projects thus enabling more data to be shared rather than kept in organisational silos.

Citizen-sensing and data-driven participation projects strengthen trust and community engagement, while making government more effective.

City councils are giving people more direct control over how data about their lives is being used. They have done this by providing citizens with simple technical tools that allow data to be collected and shared on the users' terms. Examples like the citizen-sensing of damp houses in Bristol and noise pollution in Plaza del Sol, or the use of participatory democracy platforms such as Decidim in Barcelona, encourage community cohesion, empower participants with new knowledge, and provide the council with new information so they can better understand the extent of problems faced by local people.

Section 3

Lessons for city governments

Taken together, the range of initiatives which we have outlined above paint a broad picture of practical actions policymakers are taking to build an alternative version to the smart city - one which promotes ethical data collection practices and promotes responsible innovation with new technologies. These policy actions will also be important in creating the conditions which make it possible to implement DECODE in both the pilot cities and elsewhere.

We have brought together a set of eight key lessons from our research. These are based both on our observations from what is written above, but they also describe where some of the gaps are, as expressed by our interviewees, and where more work may need to take place.

1. Build consensus around clear ethical principles, and translate them into practical policies.

The leading cities in this area define a broad mission-statement for their approach to data and responsible innovation, which helps to unify the council, service providers and the public around a clear vision. For instance, Amsterdam’s TADA manifesto hosted a range of workshops and invested in branding and public awareness to help the principles gain wider legitimacy. In addition, ethical principles should be supplemented with clear details about how they can be practically implemented. Ethical digital standards in Barcelona were translated into concrete public policy directives with specific clauses directly implemented into government’s procurement processes. Seattle’s 2015 Privacy Program also illustrates how foundational ethical principles about the management and collection of personal data can be translated into tangible, enforceable policies and practices. These include defining roles and responsibilities for privacy across the council, and creating better internal processes for auditing, reviewing and transparently publishing privacy impact assessments for data collected across departments.

2. Train public sector staff in how to assess the benefits and risks of smart technologies:

Local governments often lack expertise in how to assess the implications of data-driven technologies. This knowledge gap means that city councils need to prioritise internal capacity building initiatives. Again, Seattle is a good example of a city that is responding directly to this challenge by providing privacy-specific training to staff who work on open data. Other cities should explore this, as well as assessing the possibility of extending training more widely among council staff. This might also include training for procurement officers, or local council planning officers, who have responsibility for reviewing and approving applications for buildings or structures that include hidden sensors and cameras, but often have little understanding of the potential risks.¹⁷²



3. Look outside the council for expertise and partnerships, including with other city governments. While it's important to build internal capacity, many cities have also actively built partnerships with external organisations. Such partners can lend advice and model policies, provide technical expertise, or evaluate the impacts of new policies and programmes. For instance, advocacy groups such as the American Civil Liberties Union provided both advice and model policies which directly informed the development of the 'Privacy Localism' movement in the US. In New South Wales, Australia, the transport department has demonstrated the value of collaborating with external researchers in designing their programme to adopt differential privacy to anonymise open data. To achieve even wider impact, local governments will also need to actively start discussions with other city leaders, sharing common principles and open standards like Barcelona's ethical digital standards, which have now been shared through a GitHub repository with many other cities via the Global City CIOs Council. Other open-source tools created by the city, such as the Sentilo sensor-platform, are also being adopted by cities worldwide.

4. Find and articulate the benefits of privacy and digital ethics to multiple stakeholders. When explaining why Amsterdam has not implemented new procurement requirements for disclosing the location of privately owned sensors across the city, a senior civil servant acknowledged that it would be 'more work' for the contracting department, and that 'they don't see it as important'. In order to achieve better support for new policies, city leaders should articulate the multiple benefits that new policies will bring to people both outside and inside the council. For example, in Amsterdam the sensor register aims to both improve the transparency and accountability of private sensors located across the city, while making it less likely that data collection efforts are duplicated by the council or local entrepreneurs. Projects like Chicago's Array of Things or Zug's new e-identity system are not just about improving privacy and control for citizens, they also reduce the administrative burden of storing and managing large swathes of personal data in the public sector. To encourage engagement and support for privacy-enhancing initiatives, city leaders should focus on highlighting the tangible benefits for citizens and internal staff alike.

5. Become a test-bed for new services that give people more privacy and control. One of the most prevalent areas of innovation among city councils is the development of new identity systems for various e-government services, including the testing of decentralised alternatives that give local residents more responsibility and control over the management and use of personal data, such as Hallo.gent or Zug's uPort identity system. In Amsterdam and Barcelona, DECODE aims to provide something similar, with the addition of further anonymising features. While these projects' aims are ambitious, they are deliberately small-scale. This is because it is important for any new technology to be carefully tested in a real-world context before being rolled out more widely. For instance, each experiment is targeted at relatively isolated e-government services. In 2018, Zug will conduct an anonymous e-voting trial, as well as testing a series of other small projects which will enable citizens to rent library books, hire city bicycles, and fill in their tax forms using their uPort digital ID. Residents will need to actively volunteer to take part too. Other city governments should follow in their footsteps, finding small-scale opportunities to pilot new technologies, while being careful not to create new risks involving personal data.

6. Make time and resources available for genuine public engagement on the use of surveillance technologies.

By opening the approval process to greater public involvement and scrutiny, city governments can make local communities more active stakeholders in how decisions about the installation of potentially harmful new technologies are made. Local policymakers can learn from a range of examples here, from 'softer' measures such as the creation of simple monitoring or e-participation tools (such as Amsterdam's planned sensor register and Barcelona's Decidim platform respectively), to 'harder' measures such as the passing of new local laws that make public engagement with the installation of a new technology a legal requirement (such as Seattle's 2017 Surveillance Ordinance). The process of engagement itself should be as inclusive as possible, blending online methods as well as active outreach (see recommendation 8 below).

7. Make complex or opaque systems more understandable and accountable, while proactively building digital literacy.

There is growing concern over the means by which data is exploited to generate insights and make decisions. This includes the use of increasingly complex algorithms that are commonly designed with predictive performance rather than interpretability as a priority.¹⁷³ Here, cities could build upon the momentum of New York's task force for algorithmic transparency. Short of New York's attempts to require all source code to be made open, other cities could work towards publishing a full audit of automated decision-making tools used across different departments (the New Zealand national government recently made a similar commitment). They could also create their own plain-language descriptions of how algorithms process personal data to make decisions and conduct regular testing of these systems for bias and errors.^{iv} To complement this, local government can also play a role in supporting the development of digital literacy strategies and projects which can make both the concepts like data and algorithms more accessible to citizens. One example not mentioned above includes New York's Institute of Museum and Library Services, which grant-funded a digital privacy and data literacy training programme for library staff to teach visitors about how to protect themselves online.¹⁷⁴ Although not run by local government, it is illustrative of the kind of projects which city councils could lend support to in future.

8. Find opportunities to involve citizens in the process of data collection and analysis from start to finish.

The citizen-sensing pilots conducted in cities like Bristol and Barcelona have shown how technology projects that involve the collection and use of personal data can be firmly rooted in communities, bringing people together around a cause, while improving cohesion and digital literacy among local residents. When done correctly, this type of activity can pave the way to citizens having a much more equal relationship with governments and companies in how personal data is used. The Making Sense toolkit provides a comprehensive outline of how to design a participatory citizen-sensing pilot, and includes a range of tips to foster high quality engagement with local residents. Other cities should look to how they can anchor more of their data collection efforts around the use of these methods.¹⁷⁵

This summary is not intended to be a set of standardised policy recommendations. What other cities decide to do will of course depend on their local context and culture, so while some policy actions may be relevant it is possible that not all policies are suitable in all instances. Our intention is to provide inspiration to policymakers, and to raise awareness about interesting developments elsewhere. We also hope this will provide city policymakers with the confidence to start a conversation with colleagues about actions that they need to take in order to create a more people-centric smart city agenda that is empowering to local residents, and respectful of people's fundamental rights.

^{iv} European cities will have already begun internal efforts to improve auditing of these tools in the run up to the implementation of GDPR.

Appendix 1

Case studies



The following case studies were built using a combination of desk-based research and interviews with city government officials. We compiled two long case studies on Amsterdam and Barcelona, and six shorter case studies on New York, Seattle, San Francisco, Zug, Ghent and Sydney.

Amsterdam

Established in 2009, Amsterdam’s smart city agenda has always tried to put people at its heart, particularly through the promotion of sharing economy and peer-to-peer initiatives. Amsterdam became Europe’s first ‘Sharing City’ in 2015, and the city government proactively supports the development of sharing economy platforms and pilots.¹⁷⁶ The city’s efforts are also increasingly oriented towards the empowerment of citizens and the responsible use of personal data, and in 2018, the council’s new coalition released a progressive agenda for how the city will promote participatory democracy and data sovereignty for its residents. This agenda is the culmination of a number of projects which have tried to promote more responsible use of data in the city in recent years. These include the TADA manifesto, a register of all IoT sensors in the city, and a partnership between the Chief Technology Officer and the DECODE project.

Amsterdam’s new Municipal Coalition Agreement¹⁷⁷ includes the city’s boldest commitments to principles of data sovereignty. Released in 2018, the agreement includes a commitment to developing a Digital City Agenda, which will define concepts around ‘digital service provision and participation (modern, open government), cyber security, secure digital infrastructure and data sovereignty’.¹⁷⁸ According to the agreement, the city will aim to work with open data and open-source solutions, minimise the amount of data they collect, give citizens access to their personal data, and record the ways in which citizens can share and control their municipal government data.¹⁷⁹ In a pioneering move, it also proposes that the city ban wi-fi tracking by private companies and create an information commissioner role, who will collaborate with the city’s municipal privacy officer to ensure that ‘privacy by design’ principles are enforced in the city’.¹⁸⁰

While the plan’s action points are yet to be implemented, they do set an ambitious agenda for the new City Council, clearly establishing their commitment to principles of open and transparent governance and data sovereignty. If adhered to, this plan may help Amsterdam to unify and scale its privacy-oriented initiatives which, to date, have been splintered across different public bodies and organisations.

TADA

One such initiative is the TADA manifesto, a set of principles designed to guide the responsible use of data in digital cities. TADA was developed by the Amsterdam Economic Board (AEB), an independent organisation which facilitates a network of academic, private sector and government actors, who collaborate to improve the city and tackle key challenges in the region. In 2017, the AEB brought together a group of citizens and representatives from government, NGOs and business to create a set of six principles which companies, cities and other organisations can use to guide their use of citizens’ personal data. Smart cities, the manifesto suggests, should be inclusive and tailored to the people (including the right to be ‘digitally forgotten’), treat data generated by companies as a common good, give citizens control over both the use of their personal data and the design of their city, and maintain transparency around their collection and use of data.¹⁸¹ To make these principles more tangible for the general public, the AEB created the ‘TADA!’ brand and ‘label’, which is designed to clearly communicate that a piece of technology, event or organisation adheres to the six principles.¹⁸² The Board will also spread awareness by giving the TADA manifesto a platform at their annual We Make the City Festival.¹⁸³

The TADA manifesto serves as an example of how an organisation can take a proactive approach towards engaging cross-sectoral stakeholders - including citizens - and spreading awareness around personal data privacy and sovereignty. As of May 2018, the manifesto has 180 signatories from citizens, business leaders, academics and government representatives in the region.¹⁸⁴

If adopted by the municipal government, Koeman acknowledges that the TADA manifesto has the potential to reshape Amsterdam's procurement strategy and data policy models.¹⁸⁵ While the Council's new coalition has committed the city to implementing the six principles of the TADA manifesto, there are no details about how this will happen.

If other cities begin to adopt ethical frameworks like TADA and establish their own 'rules' about the use of data, it will be important to consider the implications for multinational companies and organisations that work across the world. Ger Baron, Amsterdam's Chief Technology Officer (CTO), notes that *"rules and regulations are very local, and companies are global. So if every city has its own policy, it's not going to work. We need to create a scale of cities that agree on basic principles"*.¹⁸⁶ For such ethical frameworks to achieve widespread impact, it may be necessary for cities to share common principles around the handling and use of personal data.

Sensor Register

Public sensors and IoT devices proliferate in smart cities, and it can be challenging for local government to keep track of where they are or why they exist. As a result, their capacity to protect residents against unnecessary or unlawful surveillance is drastically reduced. In Amsterdam, the Chief Technology Officer's Innovation Team is currently compiling a registry of all IoT devices in the city, with the aim of boosting economic development and building transparency around the use and collection of sensor data in the city.¹⁸⁷

The public register will include information about the type of IoT devices and their location, as well as the type of data they collect. Entrepreneurs will be able to access this information and request permission to use the data by contacting the owner

(who remains anonymous), and citizens will be able to file objections about particular sensors with the municipality.¹⁸⁸ By June 2018, the Council aims to have a proof of concept, and will test the feasibility of the registry over the following two years.¹⁸⁹

The successful implementation of the sensor register project requires accurate and comprehensive data on the location of sensors in the city. Accessing this data will be a key challenge for the city council, as companies may be reluctant - or unable - to reveal information about the location of their sensors and the type of data they collect. Theo Veltman from Amsterdam's Chief Technology Office says: *"We have several indications that most companies don't know where the sensors are -- because they're scattered around companies. One department has a couple, the other has a couple, and so on"*.¹⁹⁰ Indeed, Veltman also acknowledges that the possible reluctance of companies to reveal information to competitors may limit the success of the register.¹⁹¹

Mandating transparency around sensor location will be difficult to enforce, meaning that the project will begin on a voluntary basis. In future, registration on the sensor inventory may become a planning requirement for organisations wishing to install a public sensor in the city, but Veltman argues that the process of enforcing these requirements will be an ongoing challenge for the Council.¹⁹²

Holiday rental register

The Amsterdam City Council is also partnering with DECODE on a pilot project involving holiday rentals in the city. In response to growing concerns about the impact of private holiday rentals on cities, Amsterdam has introduced strict rules to regulate the letting of private properties to tourists. Landlords who wish to let their property through platforms such as AirBnb are only permitted to do so for a maximum of 60 days per year, and must list their property on an online holiday rental registry with the council.¹⁹³

DECODE technology will enable accommodation providers to share occupancy data with the municipal government in a more privacy-friendly way. The technique being developed, known as 'Attribute Based Credentials', lets users choose to reveal selected 'attributes' about themselves rather

than their full identities when interacting with council services. These could instead be simple pieces of information such as ‘this person is over the age of 18’ or ‘this person is a resident of the city of Amsterdam’.

Using the attribute-based DECODE wallet, landlords will be able to register their holiday rentals with the council whilst sharing only essential information about their property and tenants. Aik van Eemeren from Amsterdam’s Chief Technology Office highlights the need for a more secure, attribute-based interface with the rental register: *“We collect too much information now, but there is no other way. It’s a technical solution to enable data minimalism on this. That’s not there yet, and we need it”*.¹⁹⁴ If successful, the city will gain confidence and experience with technology that has in-built privacy by design and affords users more control over the sharing of personal data.

However, Job Spierings from the Waag - the organisation leading the Amsterdam pilots for DECODE - acknowledges that they may face challenges on legal, operational and political grounds when implementing the pilot. During initial user testing of a mock-up application, they also found many users were unclear about relatively basic concepts in data sharing. Within government it is considered obvious that, for instance, the tax office cannot simply lookup medical data for a taxpayer - there are several walls separating branches of government and the tax office needs to obtain multiple approvals to access this information.

The authentication interfaces that people are used to (like DigiD) actively hide these exchanges of data in favour of a simple user experience. This means citizens simply assume government has huge data lakes and have a ‘working assumption’ on what the data is used for. In that frame it is not immediately obvious why the municipality needs people to share the address of their residence (‘surely they know where to find me if I don’t pay my taxes’). In other words: giving people control of personal data can

only be done if they develop knowledge about what that control actually entails, and the UI/UX should function in ways that develop people’s agency and insight. Users became more engaged when they had the benefits and functionality of the DECODE wallet clearly explained to them.¹⁹⁵





Barcelona

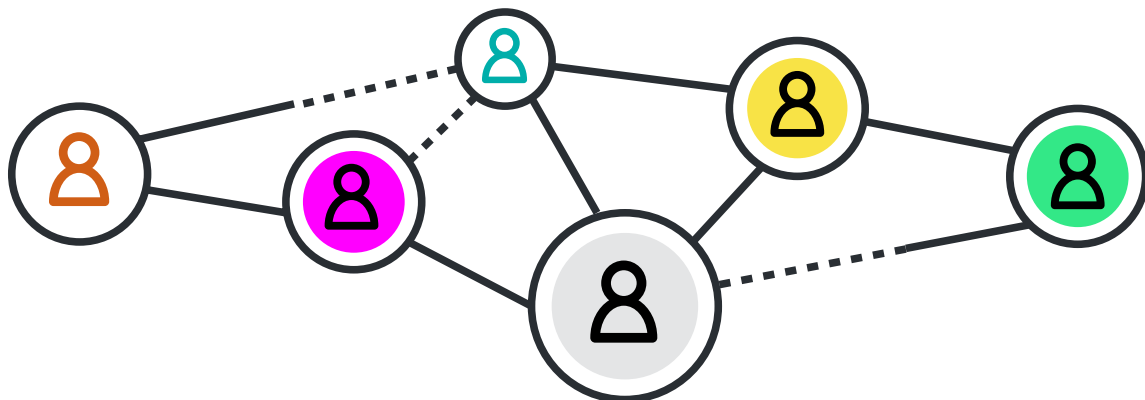
Barcelona is one of the most internationally renowned examples of a smart city. Concerted efforts to build this infrastructure began in 2011 to 2012 when the City Council worked jointly with the Municipal Institute of Informatics (IMI) to create a Smart City Strategy. This involved the launch of 122 projects organised in 22 programmes, including installation of a dedicated network of sensors to monitor noise pollution across the city; smart parking spots to indicate whether spaces are occupied or vacant; smart irrigation and waste management systems; and sensors for a variety of measurements related to air, temperature, humidity and transportation (including people and bicycle flow).¹⁹⁶

However, in 2015 the local administration changed hands. Ada Colau was elected as Mayor on a mandate of radical democratisation. The dedicated Smart City Department, along with a handful of projects, were disbanded.¹⁹⁷ But rather than putting a halt on the smart city agenda completely, the focus shifted. The Mayor nominated a new Digital Commissioner as part of the Government to rethink

and shape a new digital city strategy from the ground up to serve citizens.

Francesca Bria, the council's Chief Technology Officer told us that it wasn't always clear how smart city projects were benefiting local residents: *"one of the problems we had with the previous smart city agenda was that being technology-led and tech vendor-led meant that you end up solving lots of technology problems, instead of urban challenges and real needs that citizens have"*.¹⁹⁸

A core part of the new digital transformation agenda has been to create a cultural shift in how the council thinks about technology and data. The council's dedicated data strategy acknowledges that data has tremendous value - it can help government better understand society's needs and help them to design more responsive services. However, as more and more urban services become data driven, the question of who controls and has access to data brings data major political and ethical dilemmas: *"the question of data is at the core of who owns what in the smart city, so who is controlling what"*.¹⁹⁹



A core part of the new strategy therefore conceives of 'data as a commons', akin to a new kind of public infrastructure. This includes management data, open data, official statistics and external data collected by third parties within public spaces, or on behalf of the city.

The strategy recognises that a lot of the information collected in cities is, or can easily become, personal data, and therefore the council has a duty to shift the power to control personal data to citizens themselves, and to set the ethical digital standards

for accessing the use of this information. This includes the enforcement of appropriate privacy protections for citizens, while also providing tools that allow people to have more control over data: 'the role of the city is to be a custodian for the rights of citizens related to data.'²⁰⁰

This strategy, Bria believes, is the only way to ensure that data is harnessed in a way that can best reflect the needs of society, rather than falling into the hands of a few unaccountable actors who appropriate information for their own gain.



Ethical Digital Standards

Procurement

Barcelona has also launched a renewed procurement process for technology services. The city has changed contracting rules to incentivise responsible innovation with data and respect for privacy in the wider economy.

The council has expressed, for instance, a preference for free software, rather than proprietary software, which the council claims will help to open up competition and avoid reliance on few large technology providers.²⁰¹

Another approach has been to request that data collected by service providers that may be useful to the city must be made available to the council using open standards. The council wants to prevent the development of silos of city data, while allowing greater democratic oversight over the data being collected. According to Bria: *“more and more, data and information is the added value of the service itself, so while you are procuring services with public money, what you’re doing is a privatisation of the most important part of this service, which is who is controlling the data and the information”*.²⁰²

What’s more, by incorporating the data using open standards, city data becomes a ‘common good’ that can be used to solve city challenges. For example, the council has been negotiating with telecoms company Vodafone for a year to hand over anonymised mobility data about people living in the city. The council now has access to this data provided annually in machine readable format, and runs a programme in partnership with a local startup accelerator, running challenge prizes that involve small companies, social enterprises and cooperatives, who compete to use the data to find applications that solve local problems.

Other contracting rules require service providers to show a commitment to security and ethical data practices at every stage of the data life-cycle.²⁰³ This includes ‘privacy by design, complying with the GDPR [General Data Protection Regulation], and respecting the privacy and information self-determination of citizens.’²⁰⁴

The policy is in its early stages and it’s clear that, in the short term at least, there may be challenges

facing its implementation. Part of the issue is related to internal skills. The highest policy levels have made bold moves to declare data as a highly important asset to the council, but implementing the strategy will require a broader culture shift within the contracting department to make employees fully aware of the value, but also the risks, that ubiquitous data collection creates for people living in the city. That’s why the city has implemented a programme of training and a capability Plan for city officials to extend this kind of knowledge.

Free software and open-source technology stack for urban platforms

Many of Barcelona’s bold moves to embed data sovereignty at the heart of its smart city strategy - from procurement to citizen-sensing - are built around the open-source technologies that the city has adopted. Under the new administration, the city has built a clear vision for how different technical components will fit together to enable the safe collection and sharing of data for public benefit.

To start with, Barcelona’s ‘Sentilo’ was built to operate as the city’s main sensor platform, receiving real-time data from Internet of Things sensors all across Barcelona.²⁰⁵ Currently Sentilo only acts as a platform for ‘factual’ data, that is, information about the environment, air quality, noise, and so on. But Barcelona now has more ambitious plans to integrate citizen-sensed data into Sentilo. This would open the city’s official sensor platform to citizens (i.e. not just technology companies and the council), while also allowing people to share personal data more easily with the city.

While Sentilo acts as a collector of real-time sensor data, ‘CityOS’ acts as the city’s internal data lake - a single access-window for all datasets across the council. The city’s Chief Data Officer looks after City OS and decides who can access what. Some of the datasets are made publicly available under different degrees of openness via APIs. Currently the platform is entering the final stages of production and a range of new datasets are being added, some of which will be available via publicly accessible tools, such as via Decidim, the city’s official digital democracy portal, and a user-friendly data dashboard called BCNow (more on these below).

An important feature for each of these components is the use of free software and open standards. A problem for smart cities is that technology vendors often build proprietary solutions, which can become technological 'silos' that make the council reliant on private technology providers. By only using free software components and open standards Barcelona encourages interoperability between different software projects across the council.²⁰⁶ It also means that the council is able to require that sensor manufacturers and other companies provide their data in a format that the council understands. This isn't necessarily about privacy or data protection, but it is about creating incentives so that more city data can be made available for public benefit.

Practical tools for data sovereignty

The city's most radical ambition is to find ways that directly empower citizens with data, giving them practical tools to protect their privacy, and them let them decide exactly how that data may be used by the city council and by third parties. According to Bria *"we are not building a panopticon, it's not something that is top down decided by governments that have full access and own all of the data and decide everything ... We want to integrate personal data in terms that are transparent, ethical and secure for the citizens and where they are the ones that own this"*.²⁰⁷

As part of the DECODE project, a European Commission-funded project led by Bria, the council aims to use Decidim as a testing ground for a range of new privacy preserving features, enabling safe methods for sharing personal data. The hope is that these pilots will pave the way to citizens having a much more equal relationship with governments and tech companies in how personal data is used, and that in turn society will benefit more from access to personal data shared for the public good.

DECODE technology allow citizens to attach specific permissions to personal data, such as who may access the data and for what purpose. For example, citizens can use the Decidim platform - which currently has around 30,000 users - to propose ideas, run surveys, take part in the city's annual participatory budgeting process, or participate in consultations organised by local councillors. But many in the Decidim community have expressed concern that sharing their views on the platform will expose their political affiliations to the council, or to future administrations.²⁰⁸ Therefore DECODE will

allow users to sign petitions and engage in debates anonymously using a DECODE application. They will also be able to set specific permissions over what types of data they share (regarding age, gender and location).

Another DECODE pilot will create simple tools that allow people to collect data from within their neighbourhoods about noise and environmental pollution, as well as providing simple visualisation tools for citizens (known as the 'BarcelonaNow' dashboard), allowing citizen-sensed data to be displayed and blended with a range of other information sources - including administrative open data, and other personal information. These will be developed in ways that provide strong privacy and anonymisation protections, and control for users when they collect and share data. For instance, from these dashboards, citizens will be set permissions about who has access to personal data, for how long and for what purpose using DECODE integrated functionality.²⁰⁹

Despite the city's ambitious plans, it has been a challenge to persuade council staff about the benefits of data that is collected by the citizens themselves. Initially the council was highly sceptical about the reliability of the data. According to Mara Balestrini from Ideas for Change, who is helping to design one of the citizen-sensing pilots: *"I see that the city council feels threatened by the citizen and as usual what they do is try to defend themselves. And what they will say - they always say - is that your data is not accurate. You have to acquired this data through the means that you are supposed to acquire it. They often say: we are the experts, you are not an expert."*²¹⁰

It took a change in Government and the nomination of a new Digital Commissioner to make the case, but the council is now persuaded about the benefits brought by the citizen-owned sensors' and that their reliability is accurate and worthy of their attention. According to Bria this culture within the council is now changing: *"we are going from the previous kind of [more dismissive] approach to empowering citizens and understanding the value of their data."* The council is now exploring what it means to jointly create policies and actions with the city, and is taking a more open-minded approach to learn from, and respond more effectively, to what citizens are doing. The current government recognises it is positive to facilitate citizens' collective actions to pressure governments to change.²¹¹



New York

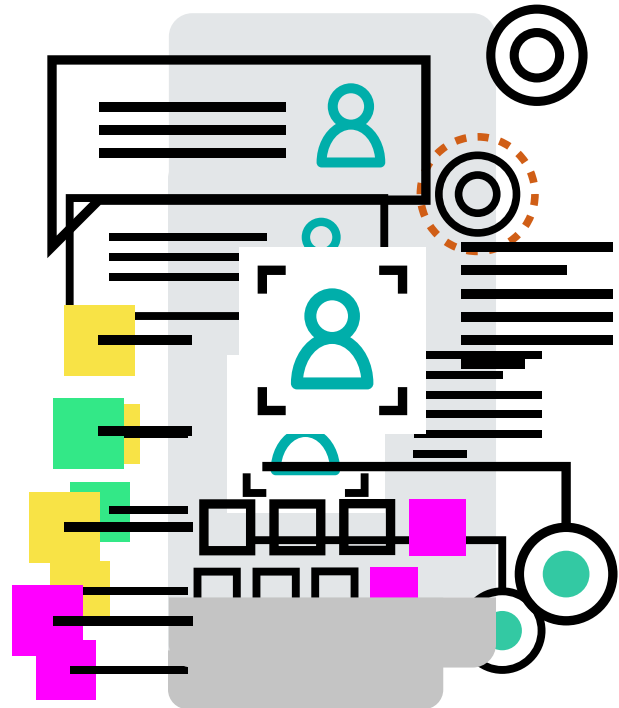
In recent years, New York City has pioneered a range of policy initiatives designed to promote the responsible use and handling of citizens' personal data. Geoff Brown, New York's Citywide Chief Information Security Officer, has acknowledged the importance of responsible data usage and privacy within the current administration: *"Protecting citizens' data while also strengthening transparency and open government has always been a priority"*.²¹² In 2018, the city appointed its first Chief Privacy Officer, Laura Negrón, who will provide guidance to municipal agencies and establish protocols around the collection, disclosure and retention of citizens' data.²¹³ When announcing Negrón's appointment, Mayor Bill de Blasio reaffirmed that New York *"is taking comprehensive measures to protect the privacy of personal information"*.²¹⁴

One such measure is the city's 'Guidelines for the Internet of Things' policy framework,²¹⁵ which was released by the Mayor's Office of Technology and Innovation in 2016.²¹⁶ The guidelines were developed to assert privacy standards around the deployment of IoT devices which use city assets or are installed in public spaces.²¹⁷ They are designed to support pre-existing privacy laws, and cover five areas: privacy and transparency; data management; infrastructure; security; and operations and sustainability.²¹⁸ For example, the guidelines assert that IoT devices should only collect data for 'explicit and legitimate' purposes, all personally identifiable information should be anonymised, and that city agencies should keep an inventory of IoT devices.²¹⁹

The IoT Guidelines are designed to encourage consistent practices across city agencies, help municipal officials understand and mitigate the risks associated with IoT deployments, and provide transparency to both the private sector and general public about the city's IoT policies.²²⁰ In a pilot project, the New York Parks Department applied the framework when installing a 'smart' park bench which counts citizen-users. Use of the framework led to the implementation of wide-ranging measures, such as the creation of a data ownership and management agreement with the smart bench

vendor.²²¹ However, while the Mayor's Office of Technology and Innovation oversees the 'broad enforcement' of the IoT guidelines,²²² they do not hold the same status as privacy laws, and thus it may prove challenging to monitor compliance.

In a bold legislative move, New York has also introduced a law designed to increase transparency around the use of algorithmic decision-making systems in the city. Across the world, algorithms are increasingly used to determine everything from school allocations to eligibility for bank loans. The proliferation of such systems in both public and private sectors has led to growing concerns about the potential impact of algorithmic bias on citizens' lives. Journalistic investigations, such as ProPublica, and academic research have found evidence of racial disparities in algorithms which are used by the US criminal justice system to assess defendants' likelihood of re-offending, and thus their eligibility for release.²²³ There is academic work which challenges these findings, but it suggests that bias or fear of bias (even if unwarranted), can stymie a potentially helpful scheme.²²⁴



In 2017, New York City Council member, James Vacca, introduced a bill calling for the establishment of a task force to monitor New York city agencies' use of automated decision-making systems. *"If we're going to be governed by machines and algorithms and data,"* Vacca said, *"they better be transparent"*.²²⁵ After multiple revisions, the bill was passed through the City Council and became law in January 2018. The task force will be responsible for publishing a report in December 2019, which will outline recommendations about the use of agency automated decision systems in the city.

More specifically, the task force will recommend procedures which will help the city to identify systems which disproportionately affects particular demographic groups, and address instances where a citizen is harmed by such a system.²²⁶ This will include procedures which give citizens the right to an explanation of such decisions and the right to contest them.²²⁷ The task force will also need to develop a procedure for making information about automated-decision making systems public, including technical information where appropriate.²²⁸ Finally, the report will assess the feasibility of a procedure for archiving these systems and their data.²²⁹

The task force was announced by Mayor Bill de Blasio in May 2018, and includes officials from city agencies and the administration, representatives from affected citizen groups, and academic experts in the field of automated systems.²³⁰ It will be co-chaired by Emily Newman, the Acting Director of the Mayor's Office of Operations, and Brittny Saunders, Deputy Commissioner for Strategic Initiatives at the NYC Commission on Human Rights.²³¹ Their recommendations have the potential to spearhead procedures which may create more transparency around the use and impact of algorithmic systems in New York City.

Introducing the bill, however, was not a smooth process for Vacca's team. Initially, they faced a lack of interest and engagement from city officials. As Zachary Hecht, who co-drafted the

bill, acknowledges: *"It wasn't an issue that exactly resonated with City Government. It was not something that everybody was thinking about"*. To generate interest, Vacca's team gave officials tangible examples of the impact of algorithmic decision-making systems in the city, and pitched an exclusive to the New York Times. As a result, the first Technology Committee Hearing about the bill was one of the most well-attended in recent memory.²³²

Yet the bill faced considerable opposition, and the first iteration had to be drastically scaled-back before being passed into law. Originally, the bill called for agencies to openly publish the source code of their automated decision making systems and allow members of the public to submit data to the systems for self-testing. However, at the Technology Committee Hearing, businesses and policy experts expressed concerns about the open publication of source code, which they felt could compromise businesses' proprietary information and lead to security risks in the public sector.²³³ When re-drafting the bill, Hecht acknowledges that they had to adopt a less ambitious agenda: *"we started to realise that while we felt source code should be public, it wasn't necessarily a precondition for transparency and accountability"*.²³⁴

Going forward, the task force will face several challenges. The first will be definitional, as they will need to determine what legally constitutes an automated decision-making system.²³⁵ The second is that the city does not currently have an inventory of the city's automated decision-making tools or spending on algorithmic services, which may impede the work of the task force.²³⁶ Hecht also acknowledges that there are concerns amongst some advocates that the report's recommendations will have limited impact and that the task force may only address the 'low hanging fruit'.²³⁷

Despite these challenges, it is clear that New York is pioneering a range of fresh initiatives to build a culture of accountability and transparency around the use of citizens' data, and have firmly established it as a priority on the city's strategic agenda.



Seattle

In 2013, Seattle’s Police Department faced a public backlash over their implementation of a wireless sensor network throughout the city. The network was designed to provide emergency services with their own communication network, but many were concerned that the sensors, which were attached to utility poles, could be used to surveil citizens by geo-tracking their wireless devices.²³⁸ Controversy also erupted over the Police Department’s use of aerial drones, which were grounded after local residents voiced privacy concerns.²³⁹ In the aftermath of these incidents, Seattle implemented a comprehensive municipal privacy programme, and is now considered to be a city leader in the field of data privacy.²⁴⁰

Seattle’s privacy programme was developed in 2015 in collaboration with community activist groups and ‘privacy thought leaders from academia, local companies, and private legal practice’.²⁴¹ At the core of the programme is a set of six privacy principles, which were adopted as a City Council Resolution and guide the City’s use and handling of citizens’ personal information. The principles²⁴² broadly define how Seattle should collect, use, store and share citizens’ personal data, and affirm the City’s commitment to maintaining accurate information

and valuing citizens’ privacy. Building on these ethical guidelines, a privacy statement²⁴³ provides a more detailed outline of how Seattle collects and manages citizens’ personal information, and a privacy policy²⁴⁴ sets forth the obligations and requirements of City departments.

Under the terms of the privacy policy, municipal agencies must complete privacy reviews of City programmes which have ‘potential privacy impacts’.²⁴⁵ The City makes Privacy Impact Assessments publicly available online, and municipal officials are guided through the review process with the help of a Privacy Toolkit, which was designed to help City departments adhere to the privacy principles and policies.²⁴⁶

In 2017, Seattle also issued an Ordinance which outlines a range of procedures designed to increase transparency around the city’s use of surveillance technologies. This includes the creation of an inventory of all surveillance technologies and the preparation of Surveillance Impact Reports for new technology.²⁴⁷ Examples of technology under review include Automated License Plate Recorders, which are attached to police vehicles, and Emergency Scene Cameras.²⁴⁸ That said, the Ordinance has also been criticised for broad exemptions to its definition



of what counts as a surveillance technology, including policy body cameras and various sources of video surveillance.²⁴⁹

Seattle's Privacy Programme also includes an Open Data Policy,²⁵⁰ which was developed in collaboration with various partners, including the University of Washington. This policy stipulates that government data should be 'open by preference', meaning that the City reserves the right to withhold data if it has the potential to cause privacy harms.²⁵¹ Under the policy, datasets must be reviewed for potential privacy harms prior to release, and an annual risk assessment must be performed of both the Open Data Program and Open Data Portal.²⁵² The Open Data Policy was introduced by a Mayoral Executive Order,²⁵³ which directs all city departments to adhere to the policy.

A range of municipal officials are assigned specific roles to manage the implementation of the Privacy Programme. For example, Chief Privacy Officer, Ginger Armbruster, is responsible for providing 'overall leadership and direction', while Open Data Champions manage their department's publication of Open Data.²⁵⁴

Seattle's approach illustrates how city governments can develop a comprehensive privacy ecosystem which fosters transparency and accountability across

multiple domains of the 'smart city', from open data to surveillance technologies. Notably, it also demonstrates how foundational ethical principles about the management and collection of personal data can be translated into tangible, enforceable policies and practices across a city. The first annual risk assessment conducted by the Future of Privacy Forum identified Seattle as 'a national leader in privacy program management', and scored the City a five out of six in the areas of 'Data Quality' and 'Transparency and Public Engagement'.

However, the report also identifies a number of challenges for Seattle's Privacy Programme. Significantly, the authors note that the City has limited access to specialised de-identification tools and statistical methods, such as differential privacy, meaning that their open data privacy reviews do not currently 'mitigate the full range of re-identification risks'.²⁵⁵ The report acknowledges that such tools are often not commercially available, or are 'difficult and costly to implement at scale', but that 'the City of Seattle's previous partnerships with privacy research centers may help pave a path forward for future developments in municipal de-identification strategies'.²⁵⁶ This is instructive for other cities, and points to the value of collaborating with external organisations when designing and implementing citywide privacy initiatives.

San Francisco

Open data initiatives have the potential to bolster innovation and improve public services and infrastructure. However, the publication of open data can pose a risk to citizens' privacy, as anonymised data can often be re-identified when combined with other datasets. Indeed, a study of data from the 2000 US Census found that 63 per cent of the US population can be uniquely identified based solely on their gender, date of birth and ZIP code.²⁵⁷ In one famous case from 1997, researcher Latanya Sweeney uncovered the medical records of Massachusetts Governor, William Weld, by combining a de-identified insurance dataset with public voter records.

San Francisco launched an open data platform called DataSF in 2009, with the aim of using data to improve city services. Recognising that current

privacy laws do not always prevent re-identification of anonymised data, the government released an Open Data Release Toolkit in 2016, which is designed to guide municipal officials through a risk assessment process prior to the publication of open data.

The toolkit²⁵⁸ provides a framework which helps municipal officials to assess the utility and value of publishing a dataset against potential risks to individual privacy. Using a four-step model, it helps officials to identify sensitive datasets, perform risk assessments and select privacy solutions such as data aggregation, k-anonymisation, and geo-masking. In some instances, it will recommend that a dataset remain closed. Notably, the toolkit is not used for public record datasets, and does not address privacy concerns relating to data collection or storage.²⁵⁹

By providing municipal leaders with a clear and actionable process for minimising privacy risks, the toolkit enables the city to use open data in a more responsible, privacy-preserving way. Already, the city San Francisco Public Library has used the toolkit to revise how they release data about the public's use of the library, limiting the specificity of geographical boundaries in the dataset to reduce the risk of re-identification.²⁶⁰ In other instances, the toolkit may actually enable the release of data that would otherwise remain closed, thus enabling researchers to access information that could be

harnessed for social benefit. This was the case for the San Francisco Mayor's Office of Housing and Community Development, who used the toolkit to release previously unpublished data about citizen engagement with affordable housing projects.²⁶¹ Charles MacNulty, who led this project, found that the process of working through the toolkit 'facilitated deep, meaningful discussion... and enriched the department's understanding of the privacy issue'.²⁶² The toolkit has also spread to other cities, including Durham and Seattle, US.²⁶³

Zug (Switzerland)

In order to streamline Switzerland's administrative and business processes, the Swiss government has made the development of an electronic identity (E-ID) a national priority.²⁶⁴ An e-ID will allow for the growth of digital e-government services, such as e-voting, make online identification more secure, and give citizens more control over the disclosure of their personal data.²⁶⁵ However, the Federal Council is outsourcing the development and implementation of the e-ID technology, and the current national 'SwissID' initiative is a joint venture between private corporations and banks such as Credit Suisse and UBS.

The Swiss city of Zug, a hub for blockchain startups, has independently pioneered a decentralised alternative to the SwissID project. Zug mayor, Dolfi Mueller, argues that the provision of an e-ID by private firms using centralised computer databases erodes citizens' trust: *"You have to trust the ID provider ... Use of technology like blockchain will make this feeling of trust stronger"*.²⁶⁶ In 2017, the city partnered with the Lucerne School of Business and Zurich tech firm ti&m to roll-out technology which enables Zug residents to register a digital e-identity on the Ethereum blockchain.

To create their digital identity, Zug residents must first download the uPort mobile app, which was developed by Ethereum tech company ConsenSys. After registering on the app and the Zug ID web portal, citizens must verify their identity in-person using official government documents. Once verified, they can use their encrypted uPort-ID to engage with e-government services such as online voting and bill payments, access proof of residency documents and issue e-Signatures.²⁶⁷ The

first e-ID was issued on November 15, 2017, and by February 2018, approximately 220 Zug residents had registered.²⁶⁸

Zug's blockchain-based e-ID claims to offer project offers a more secure alternative to other e-identity solutions, such as SwissID, which rely on centralised computer databases that can be susceptible to security breaches. This not only helps to build trust between citizens and government,²⁶⁹ but also minimises the infrastructure requirements for the city, which can avoid the burden of hosting a large server or database.²⁷⁰ Use of the e-ID also gives citizens more control over the disclosure of their personal data, and for service providers, facilitates compliance with GDPR, as only minimal information is exchanged between parties.²⁷¹

According to Mueller, Zug's e-ID project will only be successful if citizens accept and embrace this new form of digital identity.²⁷² For this to happen, it is incumbent on the city to showcase the tangible benefits of the e-ID through use-case pilots. In 2018, an e-voting trial will be held, as well as a series of other small projects which will enable citizens to rent library books, hire city bicycles, and fill in their tax forms using their uPort digital ID.²⁷³

While Switzerland's previous attempts to roll out a national e-ID have failed, the potential expansion of the national, corporate-backed SwissID may threaten the future of Zug's small blockchain project. As Mueller acknowledges, *"[SwissID] can exert much more pressure on people to have such a digital ID. They are Goliath, and we are David"*.²⁷⁴ The resilience of Zug's e-ID project will, in part, depend on the success of its use-case pilots and uptake with the local community.



Ghent

Many smart cities are driven by a technology-led model, where corporations assume control over citizens' personal data. The Belgian city of Ghent is pursuing an alternative model based on their 'City of People' strategy, which emphasises citizen co-creation and collaboration, views data as foundational, and uses technology as an 'enabler'.²⁷⁵ As part of this strategy, Ghent wants to create a city of 'smart citizens', who are empowered 'with technology that they own and control'.²⁷⁶

To achieve this, the city has provided citizens with an online data profile called 'Mijn Gent' ('My Ghent'), which contains a more detailed, enriched local version of Belgium's national personal data registry.²⁷⁷ The online profile allows citizens to access City resources, such as childcare and library services, while giving them full control over the management and sharing of their personal data.²⁷⁸ For example, if a citizen registers for a sports camp with their children, they can choose whether they share information about the number of people in their family.²⁷⁹

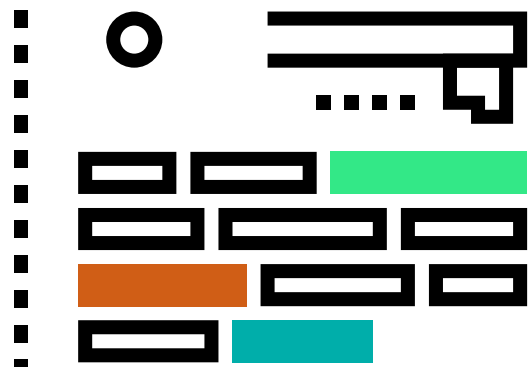
Building on the My Ghent profile, the city has been collaborating with a non-profit called Indie on an initiative called 'Hallo.gent', which aims to give Ghent citizens their own online domain and 'federated personal website' (e.g. 'JanJansen.gent').²⁸⁰ Coenegrachts describes it as like giving people their own 'piece' of the internet, like a social media profile where data and the domain itself is controlled and owned entirely by the individual citizen.²⁸¹ The aim is for Hallo.gent is to create user-friendly applications on top of the My Gent data profiles, that are 'as convenient and enjoyable to use as Facebook or Twitter'.²⁸² The system will allow the citizens to register for any council services, and council can verify different pieces of information from residents available on their own My Ghent portal, without the council ever needing to collect or store any additional personal information.

The first stage of the Hallo.gent development took place between January and April, 2018,²⁸³ and as of May 2018 there is a demonstration version of the site available.

By giving people ownership over their own 'piece' of the internet, Ghent aims to empower citizens with more individual sovereignty and control over personal data.²⁸⁴ In doing so, they are also trying to build trust between citizens and local government, as acknowledged by Ghent's Chief Strategy Officer, Karl-Filip Coenegrachts: "*City government is seen as a level of government which can still be trusted, though the trust is not there yet ... We are the only public partner able to create that trust*".²⁸⁵

In developing this project, one of the key challenges has been raising awareness around data privacy issues amongst both citizens and politicians. Going forward, the city may need to develop an operating model that can accommodate the potentially expensive process of registering individual domain names, and this may require collaboration to share the costs.²⁸⁶

In addition, while Coenegrachts argues that city governments are best placed to implement privacy solutions and policies that are responsive to local context, he also notes that the cooperation of European partners and national governments will be needed to further develop and expand the Hallo.gent initiative.²⁸⁷





Sydney

Data about public transportation services can provide valuable information to researchers and municipal officials tasked with improving city services. Yet like other forms of open data, such information can compromise citizens' privacy if 'anonymised' travel patterns are re-identified.²⁸⁸ To mitigate this risk, in March 2017, Transport for New South Wales (TfNSW)²⁸⁹ collaborated with Australia's largest data and innovation group, Data61,^v to release privacy-preserving open data about citizens' use of Sydney's public transport network.

The open dataset is a two-week sample derived from Sydney's 'tap-on, tap-off' Opal card system for public trains, buses, light rail and ferries. Recorded in July and August 2016, the data is freely downloadable and includes information about trip dates and the time and location of 'tap-ons' and 'tap-offs'.²⁹⁰ Upon its release, TfNSW's Deputy Secretary, Tony Braxton-Smith, noted that "*Opal data has long been one of our most requested and most useful datasets*" given its potential utility for both public and private organisations.²⁹¹

When releasing the Opal data, researchers applied state-of-the-art privacy protection known as differential privacy. This model is not a tool or technology, but rather a "*formal mathematical definition*"²⁹² which guarantees privacy, often by adding random 'noise' to data.²⁹³ The application of differential privacy to the Opal data means that a user's 'tap-ons' and 'tap-offs' cannot be linked or connected with their other journeys, which reduces the risk of re-identification.²⁹⁴ The time of the 'tap-ons' and 'tap-offs' have also been rounded to 15 minute intervals.²⁹⁵

New South Wales has an 'open by default' data policy, which favours the release of government data unless it is against the public interest (e.g. if the data

exposes personal information).²⁹⁶ In this instance, the application of differential privacy allowed for the data to be released for public benefit whilst preserving citizens' privacy. One analysis conducted by a researcher from the University of Technology Sydney highlighted how the data could be used to help businesses plan their opening hours and staffing arrangements around peak travel times at public transport stations.²⁹⁷ Deputy Secretary Braxton-Smith also suggested that the data "*could also help local councils, government authorities and service providers to better plan local works and services provision in the neighbourhood*".²⁹⁸

It is important to note that an academic review of the Opal dataset's privacy-preserving mechanisms, researchers found that, 'in some unusual circumstances', there is a very small probability that an attacker could detect the 'presence' of a small group or individual, but not any identifiable information.²⁹⁹ As a result, the Opal dataset "*does not technically meet the precise definition of strong Differential Privacy*", but this could be 'easily corrected' in future.³⁰⁰ Notably, the researchers used this finding to encourage openness about data privacy mechanisms, which they suggest is 'crucial for engineering good privacy protections' and 'might help improve the privacy of future releases'.³⁰¹

One drawback of privacy-preserving mechanisms is that they can often reduce the utility of a dataset.³⁰² In this instance, the application of differential privacy means that researchers cannot analyse users' trips and journeys, because their 'tap-ons' and 'tap-offs' are not linked.³⁰³ Despite this trade-off, it is clear that the release of Sydney's Opal data has the potential to yield some tangible social benefits, and illustrates how governments can apply differential privacy to safeguard citizens' personal data.

v. Data61 is a research group within Australia's Commonwealth Scientific and Industrial Research Organisation (CSIRO)

Appendix 2



DECODE Barcelona Pilots

iDigital/BCNow

This pilot partnership between Barcelona City Council and Decidim, the city’s official digital democracy platform. Local residents can use Decidim to flag up city problems, to create and sign petitions and to vote in participatory budgeting. The first part of this pilot will enable citizens to have greater control over the use of information they share when using Decidim. For example, it will also anonymous verification capabilities (such as when creating and signing local petitions) to minimise the sharing of sensitive or personally identifiable data with the city council.

The second part of the pilot will create an interactive dashboard called BCNow (BarcelonaNow), which will be linked to Decidim, and will allow a range of citizen-generated data to be aggregated and blended in a user-friendly way. BCNow aims to make data not only available to and responsibly shareable by citizens, but also useful for their purposes, by providing a visual environment populated by interactive interfaces for data exploration and visualisation.³⁰⁴

Users can create personalised dashboards and move widgets between them. For instance, they may select

the name of the data source to be visualised and additional parameters such as the time interval, the time granularity,³⁰⁵ the visual model, and the geographical granularity. The dashboard is conceived to integrate public data from Barcelona City Council sources, such as Sentilo sensor data and bikesharing data from the Municipality Open Data. In addition to these public data sources, some external data sources are integrated, such as AirBnB scraped data.³⁰⁶

In the next steps, the council plans to extend the existing data catalog with other public data sources and with users’ private data from the DECODE infrastructure to enable the creation of personalised privacy-aware visualisations. DECODE can provide means to enable visualisation of DECODE attributes with adequate sharing entitlements (public or aggregated using appropriate means) by means of a personalised, privacy-aware dashboard that merges with public data. In addition, we will allow citizens to explore data with other visual models and the underlying support of advanced data mining techniques.³⁰⁷

#MakingSense Internet of Things Pilot

The second DECODE pilot will be built on a local project, Making Sense, which was established in 2016 and has been co-funded by the European Commission. Making Sense worked with communities in Plaza del Sol to help them install sensors that measure the harmful effects of noise pollution in their neighbourhood.³⁰⁸

Building on this project, the DECODE pilot tackles the technical challenges of collating and storing a stream of citizen-sensed data, while also enabling those citizens to control what information is shared. In the pilot, residents will be given noise sensors that are placed both inside and outside of their homes. DECODE will provide sessions to train and support

participants to help them setup and use the sensors to gather and analyse data to influence city-level decisions.

This DECODE pilot will give users of these noise sensors more control over personal data by providing a secure, distributed system for IoT data access control management. It will also provide an interface to allow communities to share data with at different levels of granularity, and a wallet system for the storage of the data permissions on log-in. The ultimate aim is to enable this data to be visualised by the BCNow dashboard (see above), in order to have a unified view of all the DECODE pilots in Barcelona.



Appendix 3

DECODE Amsterdam Pilots

Gebied Online: A co-operatively owned online platform for neighbourhood communities.

Gebied Online is a pre-existing online co-operative platform which allows neighbourhood residents to come together to share events, exchange products and services, and discuss local community initiatives. The platform emerged out of a cooperatively owned website for residents of the IJburg neighbourhood in Amsterdam in 2012, and has since expanded to include five neighbourhoods and 4,000 registered citizens in the region.³⁰⁹

While Gebied Online is a citizen-led initiative, the Amsterdam City Council aims to leverage its success by partnering with the DECODE project to pilot privacy-enhancing technologies on the platform. The DECODE pilot, which will commence in 2018, will deploy a prototype application which will give residents access to a more privacy-preserving local social network, with granular controls so that residents can decide what personal data they share with the community.

For example, the DECODE application would allow users to be active in as many networks as they wish, whilst allowing them to reveal their attributes on a per network basis. A user may want to convey a different set of attributes when acting in a network in a professional capacity as when she is active in a more informal context. The first may have a different profile photo, the second may link to info on her

family. Currently this is only supported by allowing people the workaround of registering multiple times (with different email addresses).

The DECODE application would also be able to verify data when and where needed. Gebied Online is set-up as an open, transparent network with very low entry barriers, allowing (nearly) everyone to register in any community is considered a key-feature. However, in some cases it is or might be helpful to distinguish between users based on attributes, such as residency, age(group) or others. DECODE can set up a peer-to-peer verification system allowing users to prove their residency (or other demographic characteristics, such as their age group, to cryptographically prove they are recognised by their neighbours.

The application will also be able to organise secure online decision making by enabling community users to vote^{vi} when discussing priorities (among themselves or for policymakers). DECODE enables users to prioritise issues by allowing every user to participate, but in the tally of results, distinguish between results from actual residents of that community and results from 'other' participants. The pilot application would also ensure that the anonymity of each user is guaranteed.

vi. Note: this kind of 'voting' is called 'petitioning' in DECODE, to distinguish from actual electoral voting processes



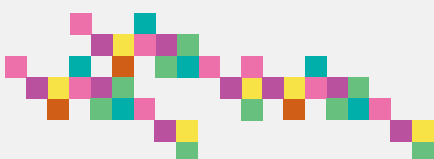
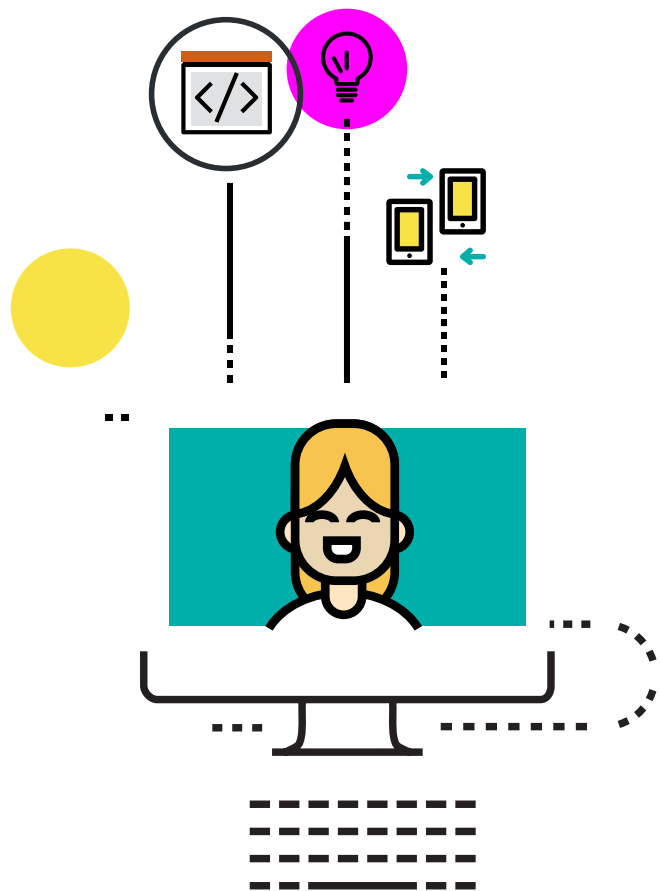
**Amsterdam register:
Municipal obligatory registration process for holiday rentals in Amsterdam**

In Amsterdam, sharing economy platforms such as AirBnB have caused disruption by pushing up the the price of rents, while legal rules around privacy have prevented effective sharing of occupancy data about hosts who break local legislation. In response to growing concerns about the impact of private holiday rentals on cities, Amsterdam has introduced strict rules to regulate the letting of private properties to tourists. Landlords who wish to let their property through platforms such as AirBnB are only permitted to do so for a maximum of 60 days per year, and must list their property on an online holiday rental registry with the council.³¹⁰

The second DECODE pilot in Amsterdam will pilot technology which will enable accommodation providers to share occupancy data with the municipal government in a more privacy-friendly way. Using the attribute-based DECODE wallet, landlords will be able to register their holiday rentals with the council whilst sharing only essential information about their property and tenants. DECODE will also provide statistics and regulatory information to enable the community to govern the platform without compromising participants' privacy.

The DECODE Wallet used in this pilot will contain a private/public keypair, and the application can either be a desktop app or mobile app. The wallet is an application that can be launched via a custom URL protocol, which passes information to the wallet. The wallet can then be used to instigate the flow and call back to the application. This way, the flow of connectivity is always only from the DECODE Wallet to the application, and the application never makes a network connection to the wallet.

If successful, the city will gain confidence and experience with technology that has in-built privacy by design and affords users more control over the sharing of personal data.



Appendix 4

DECODE Pilot Evaluation Methods

A systematic and robust impact evaluation of DECODE’s pilots is vital for the future dissemination, exploitation and scaling of DECODE’s vision and technology. It is also important for the refinement of the technology and approaches, required as the consortium create the DECODE toolkit towards the end of the project. The impact evaluation will help to articulate where and how DECODE makes a difference, and will highlight where further improvements are required.

Each pilot will develop its own impact assessment and evaluation methodologies which are specific to the focus on that pilot. These approaches will be distilled into standardised tools which can be used by other cities later on in the project. This appendix details a framework which can be used as a starting point for the development of those methodologies in the pilots and elsewhere.

Developing the DECODE Impact Assessment Strategy

To be meaningful, impact measures must be linked directly to the work of the project, the co-created focus of the pilots, and the intended final outcome of the technology, research and policy work. There are four core strands in which the work of DECODE can be categorised for impact assessment purposes:

- Pilots
- Technology
- Research
- Policy

For the purposes of impact assessment in the pilots, it is the first of these two strands which are of most relevance. It is necessary to both assess that the technology worked for the specific use case it was applied to, and the impact on a wider set of outcomes that this created.

A good impact framework should test the pilots and the technology against the specific objectives of that pilot. This requires a tailored approach to each pilot. Below is a set of steps which can be followed in order to put together a suitable framework and plan.



Stage 1 - Defining the problem to be solved

For each strand, relevant consortium partners will define the specific problems they are trying to solve.

Stage 2 - Defining objectives

For each identified problem, consortium partners will define what it would look like for this problem to be solved. These will represent statements about DECODE's objectives. The objectives will be categorised into impact types e.g. social, economic, environmental, financial.

Stage 3 - Hypothesis generation

For each objective, a hypothesis will be developed which can be used to test whether the original assumptions behind the problem and objectives were correct.

Stage 4 - Assessment criteria

The method of assessing whether an objective has been achieved will be defined. This will include identifying required datasets (including for any interim impact figures), time scales for assessment, the scale of change required to indicate impact, the methods to be used to control for counterfactuals.

Stage 5 - Plan for Assessing Impact

This will detail the allocation of responsibilities to partners, the data collection and analysis methods, time-scales, and reporting system for demonstrating impact.

Worked Example To Demonstrate Process

	STAGE 1 Problem definition	STAGE 2 Objectives definition	STAGE 3 Hypothesis	STAGE 4 Assessment criteria	STAGE 5 Plan for assessing
Pilots	People cannot share personal IOT data without risk of identification.	To give people the means to share personal IOT data without possibility of identification.	Giving people technology to share their IOT data without risk of identification will increase the number of people willing to share their personal data.	A technical proof that DECODE technology does not enable identification. Survey of users to gather views on experience of DECODE, including questions about increased likelihood to share.	Assign role of lead assessor. Lead assessor defines time-scale for assessment and arranges access to datasets. Baseline and counterfactuals are factored in.



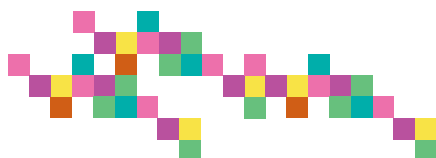
Endnotes

1. Bria, F. (2018) Our data is valuable. Here's how we can take that value back [online]. 'The Guardian.' 28 April. Available from: <https://www.theguardian.com/commentisfree/2018/apr/05/data-valuable-citizens-silicon-valley-barcelona> [Accessed 7th June 2018].
2. Hollands, R. (2008) Will the Real Smart City Please Stand Up?. 'City.' 12(3), pp.303-320.
3. Saunders, T. and Baeck, P. (2015) Rethinking Smart Cities from the Ground Up. London: Nesta.
4. Vanolo, A. (2016) Is there anybody out there? The place and role of citizens in tomorrow's smart cities. 'Futures.' 82, pp.26-36.
5. Powell, N. (2018) Sidewalk Labs pledges 'open' approach to data, but that's no guarantee they'll actually share it [online]. 'Financial Post.' 22 March. Available from: <http://business.financialpost.com/technology/sidewalk-labs-pledges-open-standard-for-data-governance-but-thats-no-guarantee-experts-say> [Accessed 19th June 2018].
6. Naafs, S. (2018) 'Living laboratories': the Dutch cities amassing data on oblivious residents [online]. 'The Guardian.' 1 March. Available from: <https://www.theguardian.com/cities/2018/mar/01/smart-cities-data-privacy-eindhoven-utrecht> [Accessed 19th June 2018].
7. Edwards, L. (2016) Privacy, security and data protection in smart cities: a critical EU law perspective. 'European Data Protection Law Review.' 2 (1), pp. 28-58.
8. See: <https://www.nrf.gov.sg/programmes/virtual-singapore> [Accessed 29/06/18]
9. Waldman, P., Chapman, L. and Robertson, J. Palantir knows everything about you [online]. 'Bloomberg Businessweek.' 23 April. Available from: https://www.bloomberg.com/features/2018-palantir-peter-thiel/?utm_medium=social&utm_campaign=socialflow-organic&utm_source=twitter&utm_content=businessweek&cmpid=socialflow-twitter-businessweek [Accessed 7th June 2018].
10. Kitchin, R. (2016) 'Getting smarter about smart cities: Improving data privacy and data Security.' Dublin: Data Protection Unit, Department of the Taoiseach.
11. Edwards, L. (2016) Privacy, security and data protection in smart cities: a critical EU law perspective. 'European Data Protection Law Review.' 2 (1), pp. 28-58.
12. Crump, C. (2016) Surveillance Policy Making by Procurement. 'Washington Law Review.' 91, pp.1595-1662.
13. Atockar (2014) 'Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset' [online]. [s.l.]: Neustar. Available from: <https://research.neustar.biz/2014/09/15/riding-with-the-stars-passenger-privacy-in-the-nyc-taxicab-dataset/> [Accessed 29th June 2018].
14. Edwards, L. and Veale, M. (2017) Slave to the Algorithm? Why a 'Right to an Explanation' is probably not the remedy you are looking for. 'Duke Law & Technology Review.' 16 (1), pp.18-84.
15. De Montjoye, Y.A., Hidalgo, C.A., Verleysen, M., Blondel, V.D. (2013) Unique in the Crowd: The privacy bounds of human mobility. 'Scientific Reports.' 3 (1376).
16. Nesta (2018) 'At the dawn of GDPR, Nesta warns it is high time for data innovation, not just regulating 'business as usual' [online]. London: Nesta. Available from: <https://www.nesta.org.uk/news/at-the-dawn-of-gdpr-nesta-warns-it-is-high-time-for-data-innovation-not-just-regulating-business-as-usual/> [Accessed 7th June 2018].
17. European Commission (2015) Special Eurobarometer 431 - Data Protection Report. Available from: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf [Accessed 7th June 2018]
18. Miller, C., Coldicutt, R. and Kos, A. (2018) 'People, Power and Technology: The 2018 Digital Attitudes Report.' London: Doteveryone.
19. p.7, Marzloff, L., Hamonic, A., & Rieg, J. (Eds.) (2017) 'Public-private partnerships in the age of data.' [s.l.]: Le Lab OuiShare x Chronos. Available from: <https://static1.squarespace.com/static/5857d136f5e2315e3e03a23c/t/59660fc44c8b0390421fde98/1499861071311/Research+2+-+Public-Private-partnerships+in+the+age+of+data+-+Research+2+-+Le+Lab+Chronos+x+OuiShare.pdf> [Accessed 20th June 2018].
20. London Assembly Transport Committee (2018) 'Future transport: How is London responding to technological innovation?' London: Greater London Authority.
21. p.7, Marzloff, L., Hamonic, A., & Rieg, J. (Eds.) (2017) 'Public-private partnerships in the age of data.' [s.l.]: Le Lab OuiShare x Chronos. Available from: <https://static1.squarespace.com/static/5857d136f5e2315e3e03a23c/t/59660fc44c8b0390421fde98/1499861071311/Research+2+-+Public-Private-partnerships+in+the+age+of+data+-+Research+2+-+Le+Lab+Chronos+x+OuiShare.pdf> [Accessed 20th June 2018].
22. Wylie, B. (2018) Sidewalk Toronto, The City of Toronto, and Our Right To Multiple Futures [online]. 'Medium.' 19 March. Available from: <https://medium.com/@biancawylie/sidewalk-toronto-the-city-of-toronto-and-our-right-to-multiple-futures-51c2778bba0b> [Accessed 7th June 2018].
23. Mattern, S. (2018) Databodies in codespace [online]. 'Places Journal.' April. Available from: <https://placesjournal.org/article/databodies-in-codespace/> [Accessed 7th June 2018].

24. Niederer, S. and Priester, R. (2016) Smart Citizens: Exploring the Tools of the Urban Bottom-Up Movement. 'Computer Supported Cooperative Work (CSCW).' 25, pp.137-152.
25. The Economist (2014) Everybody wants to rule the world. 'The Economist.' 27 November.
26. Berners-Lee, T. (2018) The web can be weaponised – and we can't count on big tech to stop it [online]. 'The Guardian.' 12 March, Available from: <https://www.theguardian.com/commentisfree/2018/mar/12/tim-berners-lee-web-weapon-regulation-open-letter> [Accessed 7th June 2018].
27. Cadwalladr, C. and Graham-Harrison, E. (2018) Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. 'The Guardian.' 17 March. Available from: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> [Accessed 19th June 2018].
28. Transport for London (2017) 'Licensing decision on Uber London Limited' [online]. London: Transport for London. Available from: <https://tfl.gov.uk/info-for/media/press-releases/2017/september/licensing-decision-on-uber-london-limited> [Accessed 7th June 2018]
29. Scheiber, N. (2017) How Uber Uses Psychological Tricks to Push its Drivers' Buttons [online]. 'The New York Times.' 2 April. Available from: <https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html> [Accessed 20th June 2018].
30. Rosenblat, A. and Stark, L. (2016) Algorithmic Labor and Information Asymmetries: A Case Study of Uber's Drivers. 'International Journal of Communication.' 10, pp. 3758-3784; Matias, J.N. (2017) 'Governing Human and machine Behavior in an Experimenting Society.' PhD Thesis, Massachusetts Institute of Technology.
31. Also see. Arrieta Ibarra, I., Goff, L., Jiménez Hernández, D., Lanier, J. and Weyl, E.G. (2017) Should we treat data as labo? Moving beyond 'free'. 'American Economic Association Papers & Proceedings.' 1(1), pp.1-5.
32. Arrieta Ibarra, I., Goff, L., Jiménez Hernández, D., Lanier, J. and Weyl, E.G. (2017) Should we treat data as labo? Moving beyond 'free'. 'American Economic Association Papers & Proceedings.' 1(1), pp.1-5.
33. For example, also see: Carballa Smichowski, B. (2016) 'Data as a common in the sharing economy: general policy proposal.' Paris: CEPN - Université Paris XIII. Available from: <https://www.scribd.com/document/327483087/Carballa-Smichowski-Bruno-2016-Data-as-a-Common-in-the-Sharing-Economy-a-General-Policy-Proposal-CEPN-WP> [Accessed 7th June 2018].
34. TransportAPI (2018) 'TransportAPI' [online]. Available from: <https://www.transportapi.com/> [Accessed 19th June 2018]; Transport for London (2017) 'TfL's free open data boosts London's economy' [online]. London: Transport for London. Available from: <https://tfl.gov.uk/info-for/media/press-releases/2017/october/tfl-s-free-open-data-boosts-london-s-economy> [Accessed 19th June 2018].
35. Eland, A. and Pope, R. (2018) A right to the digital city: A response to the Smart London 'new deal for city data' [online]. 'Medium.' 28 March. Available from: <https://medium.com/@richardjpoppe/a-right-to-the-digital-city-ce487a52353> [Accessed 7th June 2018].
36. ARUP (2016) 'Smart City Opportunities for London.' London: Greater London Authority.
37. Fuster Morell, M., Carballa Smichowski, B., Smorto, G., Espelt, R., Imperatore, P., Rebordosa, M., Rocas, M., Rodriguez, N., Senabre, E. and Ciurcina, M. (2017) 'Multidisciplinary Framework on Commons Collaborative Economy.' [s.l.]: DECODE. Available from: <https://www.decodeproject.eu/publications/multidisciplinary-framework-commons-collaborative-economy> [Accessed 19th June 2018].
38. See Siodmok, A. (2018) 'Reflecting on the LSE Executive Masters in Public Policy: A Learning Journey.' Reflective Essay Slide Deck, Civil Service Learning. Available from: https://www.slideshare.net/asiodmok/reflecting-on-the-lse-executive-masters-in-public-policy?from_m_app=ios [Accessed 7th June 2018]; Gibson, J., Robinson, M. and Cain, S. (2015) 'City Initiatives for Technology, Innovation and Entrepreneurship: a resource for city leadership.' [s.l.]: Nesta, Accenture, and Catapult Future Cities.
39. Balkan, A. (2018) 'Indienet' [online]. [s.l.]: Indienet. Available from: <https://indienet.info/> [Accessed 19th June 2018].
40. Tada.City (n.d.) 'Tada!' [online]. Available from: <https://tada.city/en/> [Accessed 12th June 2018].
41. Tada.City (n.d.) 'Tada!' [online]. Available from: <https://tada.city/en/> [Accessed 12th June 2018].
42. Koeman, W. cited in Basu, M. (2017) Amsterdam's vision for a more responsible digital city [online]. 'GovInsider.' 21 November. Available from: <https://govinsider.asia/security/amsterdam-responsible-smart-city-willem-koeman/> [Accessed: 13th June 2018]; Interview with Willem Koeman, 2 February 2018.
43. Tada.City (n.d.) 'Signatories - Tada.City' [online]. Available from: <https://tada.city/en/signatories/> [Accessed 13th June 2018].
44. GroenLinks, D66, PvdA, SP (2018) 'Coalitieakkoord / Amsterdam Municipal Coalition Agreement.' Available from: <https://www.parool.nl/rest/content/assets/61857e2a-19ae-4e12-88f4-7ccffd96377c> [Accessed 20th June 2018].
45. <https://ajuntamentdebarcelona.github.io/foss-guide/ca/Introuccio.html>
46. <https://ajuntamentdebarcelona.github.io/ethical-digital-standards-site/free-soft/0.2/introduction.html>
47. Kiley, B. and Fikse-Verkerk, M. (2013) You are a Rogue Device [online]. 'The Stranger.' 6 November. Available from: <https://www.thestranger.com/seattle/you-are-a-rogue-device/Content?oid=18143845> [Accessed 13th June 2018].

48. Kiley, B. and Fikse-Verkerk, M. (2013) You are a Rogue Device [online]. 'The Stranger.' 6 November. Available from: <https://www.thestranger.com/seattle/you-are-a-rogue-device/Content?oid=18143845> [Accessed 13th June 2018].
49. Quaintance, Z. (2018) Seattle Pushes Forward as Data Privacy Leader [online]. 'Government Technology.' 6 February. Available from: <http://www.govtech.com/data/Seattle-Pushes-Forward-as-Data-Privacy-Leader.html> [Accessed 13th June 2018]; Future of Privacy Forum (2018) 'City of Seattle Open Data Risk Assessment: Final Report.' Washington, DC: Future of Privacy Forum. Available from: <https://fpf.org/wp-content/uploads/2018/01/FPF-Open-Data-Risk-Assessment-for-City-of-Seattle.pdf> [Accessed 13th June 2018].
50. Seattle Information Technology (2018) 'About the Privacy Program' [online]. Seattle: City of Seattle. Available from: <https://www.seattle.gov/tech/initiatives/privacy/about-the-privacy-program#scope> [Accessed 13th June 2018].
51. City of Seattle (2015) 'City of Seattle Privacy Principles' [online]. Seattle: City of Seattle. Available from: <https://www.seattle.gov/Documents/Departments/InformationTechnology/City-of-Seattle-Privacy-Principles-FINAL.pdf> [Accessed 13th June 2018]
52. City of Seattle (2016) 'Open Data Policy V1.0' [online]. Seattle: City of Seattle. Available from: <http://www.seattle.gov/Documents/Departments/SeattleGovPortals/CityServices/OpenDataPolicyV1.pdf> [Accessed 13th June 2018].
53. City of Seattle (2018) 'Open Data Program' [online]. Seattle: City of Seattle. Available from: <https://data.seattle.gov/stories/s/urux-ir64> [Accessed 13th 2018].
54. City of Seattle (2016) 'Open Data Policy V1.0' [online]. Seattle: City of Seattle. Available from: <http://www.seattle.gov/Documents/Departments/SeattleGovPortals/CityServices/OpenDataPolicyV1.pdf> [Accessed 13th June 2018].
55. Murray, E.B. (2016) 'Executive Order 2016-01' [online]. Seattle: Office of the Mayor. Available from: <http://murray.seattle.gov/wp-content/uploads/2016/02/2.26-EO.pdf> [Accessed 13th June 2018].
56. Seattle Information Technology (2018) 'About the Surveillance Ordinance' [online]. Seattle: City of Seattle. Available from: <https://www.seattle.gov/tech/initiatives/privacy/surveillance-technologies/about-surveillance-ordinance> [Accessed 13th June 2018].
57. Seattle Information Technology (2018) 'Surveillance Technologies' [online]. Seattle: City of Seattle. Available from: <https://www.seattle.gov/tech/initiatives/privacy/surveillance-technologies> [Accessed 14th June 2018].
58. Buttar, S. (2017) 'West Coast Jurisdictions Advance Community Oversight of Police Surveillance' [online]. San Francisco: Electronic Frontier Foundation. Available from: <https://www.eff.org/deeplinks/2017/08/west-coast-jurisdictions-advance-community-oversight-police-surveillance> [Accessed 14th June 2018].
59. City of Seattle (2016) 'Open Data Policy V1.0' [online]. Seattle: City of Seattle. Available from: <http://www.seattle.gov/Documents/Departments/SeattleGovPortals/CityServices/OpenDataPolicyV1.pdf> [Accessed 13th June 2018].
60. Future of Privacy Forum (2018) 'City of Seattle Open Data Risk Assessment: Final Report.' Washington, DC: Future of Privacy Forum. Available from: <https://fpf.org/wp-content/uploads/2018/01/FPF-Open-Data-Risk-Assessment-for-City-of-Seattle.pdf> [Accessed 13th June 2018].
61. GroenLinks, D66, PvDA, SP (2018) 'Coalitieakkoord / Amsterdam Municipal Coalition Agreement.' Available from: <https://www.parool.nl/rest/content/assets/61857e2a-19ae-4e12-88f4-7ccffd96377c> [Accessed 20th June 2018].
62. Dovey, R. (2017) 'Two Silicon Valley Cities Get First 'Chief Privacy Officer'' [online]. Philadelphia: Next City. Available from: <https://nextcity.org/daily/entry/santa-clara-county-hires-first-chief-privacy-officer> [Accessed 13th June 2018].
63. New York City Office of the Mayor (2018) 'Mayor de Blasio Appoints Laura Negrón as Chief Privacy Officer' [online]. New York: City of New York. Available from: <http://www1.nyc.gov/office-of-the-mayor/news/167-18/mayor-de-blasio-appoints-laura-negr-n-chief-privacy-officer> [Accessed 13th June 2018].
64. City of Seattle Department of Information Technology (2015) 'City of Seattle Privacy Program' [online]. Seattle: City of Seattle. Available from: <http://ctab.seattle.gov/wp-content/uploads/2015/10/COS-Privacy-Program.pdf> [Accessed 13th June 2018].
65. Finkle, E. & DataSF (2016) 'Open Data Release Toolkit' [online]. San Francisco: DataSF. Available from: https://docs.google.com/document/d/1_K59q9ik5eEw9_-iiPCbQ8WSIGkOFovNz1uLajVHoi0/edit [Accessed 13th June 2018].
66. p.3, Finkle, E. & DataSF (2016) 'Open Data Release Toolkit' [online]. San Francisco: DataSF. Available from: https://docs.google.com/document/d/1_K59q9ik5eEw9_-iiPCbQ8WSIGkOFovNz1uLajVHoi0/edit [Accessed 13th June 2018].
67. Valenta, B. (2017) 'How San Francisco is Opening More Data with a Premium on Privacy' [online]. Cambridge, MA: Harvard Kennedy School Ash Center for Democratic Governance and Innovation. Available from: <https://datasmart.ash.harvard.edu/news/article/how-san-francisco-is-opening-more-data-with-a-premium-on-privacy-1135> [Accessed 13th June 2018].
68. Valenta, B. (2017) 'How San Francisco is Opening More Data with a Premium on Privacy' [online]. Cambridge, MA: Harvard Kennedy School Ash Center for Democratic Governance and Innovation. Available from: <https://datasmart.ash.harvard.edu/news/article/how-san-francisco-is-opening-more-data-with-a-premium-on-privacy-1135> [Accessed 13th June 2018].

69. pp.16-17, Future of Privacy Forum (2018) 'City of Seattle Open Data Risk Assessment: Final Report.' Washington, DC: Future of Privacy Forum. Available from: <https://fpf.org/wp-content/uploads/2018/01/FPF-Open-Data-Risk-Assessment-for-City-of-Seattle.pdf> [Accessed 13th June 2018].
70. p.17, Future of Privacy Forum (2018) 'City of Seattle Open Data Risk Assessment: Final Report.' Washington, DC: Future of Privacy Forum. Available from: <https://fpf.org/wp-content/uploads/2018/01/FPF-Open-Data-Risk-Assessment-for-City-of-Seattle.pdf> [Accessed 13th June 2018].
71. Crump, C. (2016) Surveillance Policy Making by Procurement. 'Washington Law Review.' 91, pp.1595-1662.
72. American Civil Liberties Union (2018) 'Community Control Over Police Surveillance' [online]. New York: American Civil Liberties Union. Available from: <https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance?redirect=feature/community-control-over-police-surveillance> [Accessed 13th June 2018].
73. Forestieri, K. (2016) Santa Clara County cracks down on police surveillance technology [online]. 'Palo Alto Online.' 20 June. Available from: <https://www.paloaltoonline.com/news/2016/06/18/county-cracks-down-on-police-surveillance-technology> [Accessed 18th June 2018].
74. Brennan Center for Justice (2017) 'The Public Oversight of Surveillance Technology (POST) Act: A Resource Page' [online]. New York: New York University School of Law. Available from: <https://www.brennancenter.org/analysis/public-oversight-police-technology-post-act-resource-page> [Accessed 28th June, 2018]; Public Oversight of Police Technology Act, 2017. New York: The New York City Council. Available from: <http://legistar.council.nyc.gov/LegislationDetail.aspx?ID=2972217&GUID=0D8289B8-5F08-4E6F-A0D1-2120EF7A0DCA&Options=ID%7CText%7C&Search=> [Accessed 28th June 2018].
75. Public Oversight of Police Technology Act, 2017. New York: The New York City Council. Available from: <http://legistar.council.nyc.gov/LegislationDetail.aspx?ID=2972217&GUID=0D8289B8-5F08-4E6F-A0D1-2120EF7A0DCA&Options=ID%7CText%7C&Search=> [Accessed 28th June 2018].
76. Seattle Information Technology (2018) 'About the Surveillance Ordinance' [online]. Seattle: City of Seattle. Available from: <https://www.seattle.gov/tech/initiatives/privacy/surveillance-technologies/about-surveillance-ordinance> [Accessed 13th June 2018]
77. Seattle Information Technology (2018) 'Comment on a Surveillance Technology' [online]. Seattle: City of Seattle. Available from: <https://www.seattle.gov/tech/initiatives/privacy/comment-on-surveillance-tech> [Accessed 13th June 2018].
78. Oakland City Council (2018) 'Oakland Surveillance and Community Safety Ordinance' [online]. San Francisco: Electronic Frontier Foundation. Available from: <https://www.eff.org/document/oakland-surveillance-and-community-safety-ordinance-20180424> [Accessed 13th June 2018].
79. Zetter, K. (2014) Police Contract with Spy Tool Maker Prohibits Talking About Device's Use [online]. 'Wired.' 3 April. Available from: <https://www.wired.com/2014/03/harris-stingray-nda/> [Accessed 13th June 2018].
80. Lecher, C. (2018) What Happens when an Algorithm Cuts Your Health Care [online]. 'The Verge.' 21 March. Available from: <https://www.theverge.com/2018/3/21/17144260/healthcare-medicaid-algorithm-arkansas-cerebral-palsy> [Accessed 19th June 2018]; Waldman, P., Chapman, L. and Robertson, J. Palantir knows everything about you [online]. 'Bloomberg Businessweek.' 23 April. Available from: https://www.bloomberg.com/features/2018-palantir-peter-thiel/?utm_medium=social&utm_campaign=socialflow-organic&utm_source=twitter&utm_content=businessweek&cmpid=socialflow-twitter-businessweek [Accessed 7th June 2018].
81. <https://science.iupui.edu/2018/03/iupui-field-data-study-finds-no-evidence-racial-bias-predictive-policing>
82. Angwin, J., Larson, J., Mattu, S. and Kirchner, L. (2016) Machine Bias [online]. 'ProPublica.' 23 May. Available from: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> [Accessed 14th June 2018].
83. Flores, A.W., Bechtel, K. and Lowenkamp, C.T. (2016) False Positives, False Negatives, and False Analyses: A Rejoinder to "Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And it's Biased Against Blacks." 'Federal Probation.' 80(2).
84. Cited in Powles, J. (2017) New York City's Bold, Flawed Attempt to Make Algorithms Accountable New Yorker [online]. 'The New Yorker.' 20 December. Available from: <https://www.newyorker.com/tech/elements/new-york-citys-bold-flawed-attempt-to-make-algorithms-accountable> [Accessed 19th June 2018].
85. Interview with Zachary Hecht, 27 March 2018.
86. Interview with Zachary Hecht, 27 March 2018.
87. Interview with Zachary Hecht, 27 March 2018.



88. Interview with Zachary Hecht, 27 March 2018.
89. Interview with Zach Hecht, 27 March 2018; Zima, E. (2018) Could New York City's AI Transparency Bill be a Model for the Country? [online]. 'Government Technology.' 4 January. Available from: <http://www.govtech.com/Could-New-York-Citys-AI-Transparency-Bill-Be-a-Model-for-the-Country.html?flipboard=yes> [Accessed 14th June 2018]; New York City Office of the Mayor (2018) 'Mayor de Blasio Announces First-In-Nation Task Force to Examine Automated Decision Systems Used by the City' [online]. New York: City of New York. Available from: <http://www1.nyc.gov/office-of-the-mayor/news/251-18/mayor-de-blasio-first-in-nation-task-force-examine-automated-decision-systems-used-by> [Accessed 14th June 2018].
90. New York City Office of the Mayor (2018) 'Mayor de Blasio Announces First-In-Nation Task Force to Examine Automated Decision Systems Used by the City' [online]. New York: City of New York. Available from: <http://www1.nyc.gov/office-of-the-mayor/news/251-18/mayor-de-blasio-first-in-nation-task-force-examine-automated-decision-systems-used-by> [Accessed 14th June 2018].
91. Interview with Zachary Hecht, 27 March 2018.
92. Powles, J. (2017) New York City's Bold, Flawed Attempt to Make Algorithms Accountable New Yorker [online]. 'The New Yorker.' 20 December. Available from: <https://www.newyorker.com/tech/elements/new-york-citys-bold-flawed-attempt-to-make-algorithms-accountable> [Accessed 19th June 2018]; Interview with Zachary Hecht, 27 March 2018.
93. Interview with Zachary Hecht, 27 March 2018.
94. Interview with Zachary Hecht, 27 March 2018.
95. Powles, J. (2017) New York City's Bold, Flawed Attempt to Make Algorithms Accountable New Yorker [online]. 'The New Yorker.' 20 December. Available from: <https://www.newyorker.com/tech/elements/new-york-citys-bold-flawed-attempt-to-make-algorithms-accountable> [Accessed 19th June 2018]; Interview with Zachary Hecht, 27 March 2018.
96. Interview with Zachary Hecht, 27 March 2018.
97. Interview with Francesca Bria, 16 April 2018.
98. Bria, F. (2018) 'Ethical and Responsible Data Management: Barcelona Data Commons' [online]. Barcelona: Ajuntament de Barcelona. Available from: <http://ajuntament.barcelona.cat/digital/en/blog/ethical-and-responsible-data-management-barcelona-data-commons> [Accessed 19th June 2018]
99. Barcelona City Council's Office for Technology and Digital Innovation (2017) 'Barcelona City Council ICT Public Procurement Guide.' Barcelona: Ajuntament de Barcelona. Available from: http://ajuntament.barcelona.cat/digital/sites/default/files/guia_adt_6_guia_de_compra_publica_tic_en_2017_af_9en.pdf [Accessed 19th June 2018].
100. Interview with Francesca Bria, 16 April 2018.
101. Interview with Malcolm Bain, 19 March 2018.
102. See for example <https://ajuntament.barcelona.cat/digital/en/blog/ethical-and-responsible-data-management-barcelona-data-commons> [Accessed 20 June 2018]
103. New York City Mayor's Office of the Chief Technology Officer (n.d.) 'FAQ - IoT Guidelines' [online]. New York: The City of New York. Available from: <https://iot.cityofnewyork.us/faq/> [Accessed 13th June 2018]
104. New York City Mayor's Office of the Chief Technology Officer (n.d.) 'IoT Guidelines' [online]. New York: The City of New York. Available from: <https://iot.cityofnewyork.us/> [Accessed 13th June 2018]
105. See: <https://iot.cityofnewyork.us/> [Accessed 19th June 2018]
106. NYC Innovation & Emerging Technologies Workgroup (2016) 'NYC Innovation & Emerging Technologies Workgroup Presents: NYC Guidelines for the Internet of Things.' PowerPoint Slide Deck, The New York State Forum. Available from https://www.nysforum.org/events/9_14_2016/9_14_16_NYCGuidelinesIoT.pdf [Accessed 13th June 2018].
107. New York City Mayor's Office of the Chief Technology Officer (n.d.) 'FAQ - IoT Guidelines' [online]. New York: The City of New York. Available from: <https://iot.cityofnewyork.us/faq/> [Accessed 13th June 2018]
108. New York City Mayor's Office of the Chief Technology Officer (n.d.) 'FAQ - IoT Guidelines' [online]. New York: The City of New York. Available from: <https://iot.cityofnewyork.us/faq/> [Accessed 13th June 2018]
109. Rubinstein, I (2018) Privacy Localism. 'NYY School of Law, Public Law Research Paper No. 18-18.'
110. Bain, M. (2014) 'Sentilo Case Study' [online]. [s.l.]: European Commission. Available from: https://joinup.ec.europa.eu/sites/default/files/document/2014-06/SENTILO%20case_joinup_v_1%202.pdf [Accessed 19th June 2018].
111. Interview with Jordi Cirera, 19 March 2018.
112. Interview with Jordi Cirera, 19 March 2018.
113. Balkan, A. (2018) 'Gent Info' [online]. [s.l.]: Indienet. Available from: <https://indienet.info/hallo.gent/meeting-notes/gentinfo/> [Accessed 19th June 2018].
114. Balkan, A. (2018) 'Indienet' [online]. [s.l.]: Indienet. Available from: <https://indienet.info/> [Accessed 19th June 2018]; Smart Circle (2013) 'City of Ghent: The Smart-Citizen is our Starting Point' [online]. [s.l.]: Euroforum. Available from: <https://www.smart-circle.org/smartcity/uncategorized/the-smart-citizen-is-our-starting-point/> [Accessed 19th June 2018].
115. Interview with Karl-Filip Coenegrachts, 3 May 2018.
116. Interview with Karl-Filip Coenegrachts, 3 May 2018.
117. Interview with Karl-Filip Coenegrachts, 3 May 2018.
118. Balkan, A. (2018) 'Hallo.gent' [online]. [s.l.]: Indienet. Available from: <https://indienet.info/hallo.gent/> [Accessed 19th June 2018].

119. Balkan, A. (2018) 'Indienet' [online]. [s.l.]: Indienet. Available from: <https://indienet.info/> [Accessed 19th June 2018]; Balkan, A. (2018) 'Hallo.gent' [online]. [s.l.]: Indienet. Available from: <https://indienet.info/hallo.gent/> [Accessed 19th June 2018].
120. Interview with Karl-Filip Coenegrachts, 3 May 2018; Balkan, A. (2018) 'Indienet' [online]. [s.l.]: Indienet. Available from: <https://indienet.info/> [Accessed 19th June 2018]
121. 'Hallo.Gent' [online]. Available from: <https://hallo.gent/> [Accessed 28th June 2018].
122. Interview with Karl-Filip Coenegrachts, 3 May 2018.
123. Balkan, A. (2018) 'Gent Info' [online]. [s.l.]: Indienet. Available from: <https://indienet.info/hallo.gent/meeting-notes/gentinfo/> [Accessed 19th June 2018]; Interview with Karl-Filip Coenegrachts, 3 May 2018.
124. eGovernment Switzerland (n.d.) 'Establishment of an electronic identity (E-ID) that is valid nationally and internationally' [online]. Berne, CH: Programme Office eGovernment Switzerland. Available from: <https://www.egovernment.ch/en/umsetzung/schwerpunktplan/elektronische-identitat/> [Accessed 19th June 2018].
125. Interview with Dolfi Mueller, 23 March 2018.
126. Interview with Dolfi Mueller, 23 March 2018; Kohlhaas, P. (2017) Zug ID: Exploring the First Publicly Verified Blockchain Identity [online]. 'Medium.' 7 December. Available from: <https://medium.com/uport/zug-id-exploring-the-first-publicly-verified-blockchain-identity-38bd0ee3702> [Accessed 19th June 2018]
127. Kohlhaas, P. (2017) Zug ID: Exploring the First Publicly Verified Blockchain Identity [online]. 'Medium.' 7 December. Available from: <https://medium.com/uport/zug-id-exploring-the-first-publicly-verified-blockchain-identity-38bd0ee3702> [Accessed 19th June 2018]
128. uPort (2017) First official registration of a Zug citizen on Ethereum [online]. 'Medium.' 15 November. Available from: <https://medium.com/uport/first-official-registration-of-a-zug-citizen-on-ethereum-3554b5c2c238> [Accessed 19th June 2018]; Cretin, A. (2018) It's 2018 – Blockchain is on its way to Become the New Internet [online]. 'Medium.' 5 January. Available from: <https://medium.com/@andrewcretin/its-2018-blockchain-is-on-its-way-to-become-the-new-internet-7055ed6851ec> [Accessed 19th June 2018].
129. Offerman, A. (2018) 'Swiss City of Zug issues Ethereum blockchain-based eIDs' [online]. [s.l.]: European Commission. Available from: <https://joinup.ec.europa.eu/document/swiss-city-zug-issues-ethereum-blockchain-based-eids> [Accessed 19th June 2018].
130. Interview with Dolfi Mueller, 23 March 2018.
131. IAmsterdam (2018) 'Renting out your Amsterdam apartment to tourists' [online]. Amsterdam: IAmsterdam. Available from: <https://www.iamsterdam.com/en/living/everyday-essentials/housing/holiday-rentals-in-amsterdam> [Accessed 19th June 2018].
132. Interview with Aik van Eemeren, 1 February 2018.
133. Culnane, C., Rubinstein, B.I.P., and Teague, V. (2017) 'Privacy Assessment of De-identified Opal Data: A report for Transport for NSW.' [s.l.]: CoRR. Available from: <https://arxiv.org/pdf/1704.08547.pdf> [Accessed 19th June 2018].
134. Transport for New South Wales is a state government agency that is responsible for transport within the city of Sydney.
135. Data61 is a research group within Australia's Commonwealth Scientific and Industrial Research Organisation (CSIRO).
136. Green, B., Cunningham, G., Ekblaw, A. Kominers, P., Linzer, A. and Crawford, S. (2017) 'Open Data Privacy.' Cambridge, MA: Berkman Klein Center. Available from: <https://dash.harvard.edu/handle/1/30340010> [Accessed 19th June 2018].
137. Braun, T., Fung, B.C.M., Iqbal, F. and Shah, B. (2018) Security and Privacy Challenges in Smart Cities. 'Sustainable Cities and Society.' 39, pp.499-507; Greenberg, A. (2017) How one of Apple's Key Privacy Safeguards Falls Short [online]. 'Wired.' 15 September. Available from: <https://www.wired.com/story/apple-differential-privacy-shortcomings/> [Accessed 19th June 2018].
138. Jameel Asghar, H., Tyler, P and Kaafar, M.A. (2017) 'Differentially Private Release of Public Transport Data: The Opal Use Case.' [s.l.]: CoRR. Available from: <https://arxiv.org/pdf/1705.05957.pdf> [Accessed 19th June 2018].
139. Government Information (Public Access) Act No 52, 2009. Sydney: Government of New South Wales. Available from: <https://www.legislation.nsw.gov.au/acts/2009-52.pdf> [Accessed 19th June 2018].
140. See <https://opendataforum.transport.nsw.gov.au/t/insight-from-our-data-simple-analysis-using-the-open-opal-data/709> [Accessed 19th June 2018].
141. Transport for NSW (2017) 'Small Business' Opal Data Boost' [online]. Sydney: Transport for New South Wales. Available from: <https://www.transport.nsw.gov.au/newsroom-and-events/media-releases/small-business-opal-data-boost> [Accessed 19th June 2018].
142. Culnane, C., Rubinstein, B.I.P., and Teague, V. (2017) 'Privacy Assessment of De-identified Opal Data: A report for Transport for NSW.' [s.l.]: CoRR. Available from: <https://arxiv.org/pdf/1704.08547.pdf> [Accessed 19th June 2018].
143. Culnane, C., Rubinstein, B.I.P., and Teague, V. (2017) 'Privacy Assessment of De-identified Opal Data: A report for Transport for NSW.' [s.l.]: CoRR. Available from: <https://arxiv.org/pdf/1704.08547.pdf> [Accessed 19th June 2018].
144. Culnane, C., Rubinstein, B.I.P., and Teague, V. (2017) 'Privacy Assessment of De-identified Opal Data: A report for Transport for NSW.' [s.l.]: CoRR. Available from: <https://arxiv.org/pdf/1704.08547.pdf> [Accessed 19th June 2018].

145. Montes Portela, C., Rooden, H., Kohlmann, J., Van Leersum, D., Geldtjeijer, D., Sloopweg, H. and Van Eekelen, M. (2013) A Flexible, Privacy Enhanced and Secured ICT Architecture for a Smart Grid Project with Active Consumers in the City of Zwolle. 'In: 22nd International Conference and Exhibition on Electricity Distribution, Conference Proceedings, 10-13 June.' Stockholm: IET.
146. Array of Things (2016) 'Array of Things' [online]. Chicago: Array of Things. Available from <https://arrayofthings.github.io/> [Accessed 19th June 2018].
147. Array of Things (2016) 'Array of Things FAQ' [online]. Chicago: Array of Things. Available from <https://arrayofthings.github.io/faq.html> [Accessed 19th June 2018].
148. Seattle Information Technology (2018) 'Surveillance Technologies' [online]. Seattle: City of Seattle. Available from: <https://www.seattle.gov/tech/initiatives/privacy/surveillance-technologies> [Accessed 14th June 2018].
149. Seattle Information Technology (2018) 'Surveillance Technologies' [online]. Seattle: City of Seattle. Available from: <https://www.seattle.gov/tech/initiatives/privacy/surveillance-technologies> [Accessed 14th June 2018].
150. Veltman, T. 15th March 2018 'Amsterdam Sensor Registry.' email correspondence.
151. Interview with Theo Veltman, 25 April 2018.
152. Interview with Theo Veltman, 25 April 2018.
153. Interview with Theo Veltman, 25 April 2018.
154. Interview with Theo Veltman, 25 April 2018.
155. Miyazaki, M. and Hayano, R. (2017) Individual external dose monitoring of all citizens of Date City by passive dosimeter 5 to 51 months after the Fukushima NPP accident (series): 1. Comparison of individual dose with ambient dose rate monitored by aircraft surveys. 'Journal of Radiological Protection.' 37, pp. 1-12.
156. Christchurch City Council (n.d.) 'Sensibel' [online]. Christchurch: Christchurch City Council. Available from: <https://ccc.govt.nz/the-council/future-projects/smart-cities-programme/sensibel/> [Accessed 19th June 2018].
157. CRCSI (2018) '4.49 Sensing the City' [online]. Melbourne: CRCSI. Available from: <http://www.crcsi.com.au/research/4-4-health/current-projects/4-49-sensing-the-city/> [Accessed 19th June 2018].
158. Interview with Francesca Bria, 16 April 2018.
159. Interview with Francesca Bria, 16 April 2018.
160. Figures taken from: <https://waag.org/sites/waag/files/2018-03/decode-presentation.pdf> [Accessed 20 June 2018]
161. <http://bcnnow.decodeproject.eu/>
162. Marras, M., Manca, M. and Laniado, D. (2017) 'Creating interactive visualisations to make sense of city data' [online]. London: DECODE / Nesta. Available from: <https://www.decodeproject.eu/blog/creating-interactive-visualisations-make-sense-city-data> [Accessed 19th June 2018].
163. Marras, M. and Laniado, D. (2018) 'BarcelonaNow at "The Web Conference 2018"' [online]. London: DECODE / Nesta. Available from: <https://www.decodeproject.eu/blog/barcelonanow-%E2%80%9Cweb-conference-2018%E2%80%9D> [Accessed 18th June 2018].
164. Interview with Francesca Bria, 16 April 2018.
165. Knowle West Media Centre (2016) 'The Bristol Approach in action.' Bristol: Knowle West Media Centre. Available from: https://issuu.com/knowlewestmedia/docs/bristol_approach_booklet_issu [Accessed 19th June 2018]
166. Interview with Mara Balestrini, 20 March 2018.
167. Interview with Mara Balestrini, 20 March 2018.
168. Balestrini, M., Rogers, Y., Hassan, C., Creus, J., King, M. and Marshall, P. (2017) A City in Common: A Framework to Orchestrate Large-scale Citizen Engagement around Urban Issues. 'In: CHI '17: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, 7 -11 May 2017.' New York: Association for Computing Machinery (ACM).
169. Making Sense (n.d.) 'Plaza del Sol' [online]. [s.l.]: Making Sense. Available from: <http://plazadelsof.cat/> [Accessed 19th June 2018].
170. Making Sense (2018) 'Citizen Sensing: A Toolkit.' [s.l.]: Making Sense. Available from: <http://making-sense.eu/wp-content/uploads/2018/01/Citizen-Sensing-A-Toolkit.pdf> [Accessed 19th June 2018].
171. P.16 Making Sense (2018) 'Citizen Sensing: A Toolkit.' [s.l.]: Making Sense. Available from: <http://making-sense.eu/wp-content/uploads/2018/01/Citizen-Sensing-A-Toolkit.pdf> [Accessed 19th June 2018].
172. Pope, R. (2018) 'A model planning condition for digital infrastructure' [online]. Available from: <https://blog.memespring.co.uk/2018/01/30/a-model-planning-condition/> [Accessed 19th June 2018]; Nesta (2018) 'City Data Conference: from Analytics to AI' [online]. London: Nesta. Available from: <https://www.nesta.org.uk/event/city-data-conference-analytics-ai/> [Accessed 19th June 2018].
173. Edwards, L. (2016) Privacy, security and data protection in smart cities: a critical EU law perspective. 'European Data Protection Law Review.' 2 (1), pp. 28-58.
174. Data Privacy Project (n.d.) 'Learning Modules: Overview' [online]. New York: Data Privacy Project. Available from: <https://dataprivacyproject.org/learning-modules/overview/> [Accessed 19th June 2018]; Data Privacy Project (n.d.) 'Privacy Literacy Training' [online]. New York: Data Privacy Project. Available from: <https://dataprivacyproject.org/initiatives/privacy-literacy-training/> [Accessed 19th June 2018].
175. Making Sense (2018) 'Citizen Sensing: A Toolkit.' [s.l.]: Making Sense. Available from: <http://making-sense.eu/wp-content/uploads/2018/01/Citizen-Sensing-A-Toolkit.pdf> [Accessed 19th June 2018].



176. Amsterdam Smart City (2016) 'Sharing Economy' [online]. Amsterdam: Amsterdam Smart City. Available from: <https://amsterdamsmartcity.com/projects/sharing-economy> [Accessed 20th June 2018]; shareNL (2016) 'Amsterdam actionplan sharing economy.' Slide deck. Available from: <https://www.slideshare.net/shareNL/amsterdam-actionplan-sharing-economy> [Accessed 19th June 2018].
177. GroenLinks, D66, PvdA, SP (2018) 'Coalitieakkoord / Amsterdam Municipal Coalition Agreement.' Available from: <https://www.parool.nl/rest/content/assets/61857e2a-19ae-4e12-88f4-7ccffd96377c> [Accessed 20th June 2018].
178. p.58, GroenLinks, D66, PvdA, SP (2018) 'Coalitieakkoord / Amsterdam Municipal Coalition Agreement.' Available from: <https://www.parool.nl/rest/content/assets/61857e2a-19ae-4e12-88f4-7ccffd96377c> [Accessed 20th June 2018].
179. GroenLinks, D66, PvdA, SP (2018) 'Coalitieakkoord / Amsterdam Municipal Coalition Agreement.' Available from: <https://www.parool.nl/rest/content/assets/61857e2a-19ae-4e12-88f4-7ccffd96377c> [Accessed 20th June 2018].
180. GroenLinks, D66, PvdA, SP (2018) 'Coalitieakkoord / Amsterdam Municipal Coalition Agreement.' Available from: <https://www.parool.nl/rest/content/assets/61857e2a-19ae-4e12-88f4-7ccffd96377c> [Accessed 20th June 2018].
181. TADA.City (n.d.) 'TADA!' [online]. Available from: <https://tada.city/en/> [Accessed 12th June 2018].
182. Koeman, W. cited in Basu, M. (2017) Amsterdam's vision for a more responsible digital city [online]. 'GovInsider.' 21 November. Available from: <https://govinsider.asia/security/amsterdam-responsible-smart-city-willem-koeman/> [Accessed: 13th June 2018]; Interview with Willem Koeman, 2 February 2018.
183. Interview with Willem Koeman, 2 February 2018.
184. TADA.City (n.d.) 'Signatories - TADA.City' [online]. Available from: <https://tada.city/en/signatories/> [Accessed 13th June 2018].
185. Interview with Willem Koeman, 2 February 2018.
186. Interview with Ger Baron, 2 February 2018
187. Veltman, T. 15th March 2018 'Amsterdam Sensor Registry.' email to T.Bass.
188. Veltman, T. 15th March 2018 'Amsterdam Sensor Registry.' email to T.Bass.
189. Interview with Theo Veltman, 25 April 2018.
190. Interview with Theo Veltman, 25 April 2018.
191. Interview with Theo Veltman, 25 April 2018.
192. Interview with Theo Veltman, 25 April 2018.
193. IAmsterdam (2018) 'Renting out your Amsterdam apartment to tourists' [online]. Amsterdam: IAmsterdam. Available from: <https://www.iamsterdam.com/en/living/everyday-essentials/housing/holiday-rentals-in-amsterdam> [Accessed 19th June 2018].
194. Interview with Aik van Eemeren, 1 February 2018.
195. DECODE (2018) 'User feedback Decode mock-up (Amsterdam Register, January 2018).' DECODE, unpublished.
196. Moskvitch, K. (2016) Barcelona: The World's Smartest City? 'E&T Magazine.' June, pp. 48-51; Sinaeepourfard, A., Garcia, J., Masip-Bruin, X., Marin-Torder, E., Cicera, J., Grau, G. and Casaus, F. (2016) Estimating Smart City Sensors Data Generation Current and Future Data in the City of Barcelona. 'In: The 15th IFIP Annual Mediterranean Ad Hoc Networking Workshop, Conference Proceedings, June 20-21.' Barcelona: [n.k.]
197. Moskvitch, K. (2016) Barcelona: The World's Smartest City? 'E&T Magazine.' June, pp. 48-51.
198. Interview with Francesca Bria, 16 April 2018.
199. Bria, F. (2018) 'Ethical and Responsible Data Management: Barcelona Data Commons' [online]. Barcelona: Ajuntament de Barcelona. Available from: <http://ajuntament.barcelona.cat/digital/en/blog/ethical-and-responsible-data-management-barcelona-data-commons> [Accessed 19th June 2018]; Interview with Francesca Bria, 16 April 2018.
200. Interview with Francesca Bria, 16 April 2018.
201. Barcelona City Council's Office for Technology and Digital Innovation (2017) 'Code of Technological Practices for Barcelona City Council.' Barcelona: Ajuntament de Barcelona. Available from: http://ajuntament.barcelona.cat/digital/sites/default/files/guia_adt_2_codi_de_practiques_tecnologiques_en_2017_af_9en.pdf [Accessed 19th June 2018].
202. Interview with Francesca Bria, 16 April 2018
203. Barcelona City Council's Office for Technology and Digital Innovation (2017) 'Barcelona City Council ICT Public Procurement Guide.' Barcelona: Ajuntament de Barcelona. Available from: http://ajuntament.barcelona.cat/digital/sites/default/files/guia_adt_6_guia_de_compra_publica_tic_en_2017_af_9en.pdf [Accessed 19th June 2018].
204. Interview with Francesca Bria, 16 April 2018
205. Interview with Jordi Cirera, 19 March 2018.
206. Bain, M. (2014) 'Sentilo Case Study' [online]. [s.l.]: European Commission. Available from: https://joinup.ec.europa.eu/sites/default/files/document/2014-06/SENTILO%20case_joinup_v_1%20202.pdf [Accessed 19th June 2018].
207. Interview with Francesca Bria, 16 April 2018
208. Figures taken from: <https://waag.org/sites/waag/files/2018-03/decode-presentation.pdf> [Accessed 20 June 2018]
209. Marras, M., Manca, M. and Laniado, D. (2017) 'Creating interactive visualisations to make sense of city data' [online]. London: DECODE / Nesta. Available from: <https://www.decodeproject.eu/blog/creating-interactive-visualisations-make-sense-city-data> [Accessed 19th June 2018].

210. Interview with Mara Balestrini, 20 March 2018.
211. Interview with Francesca Bria, 16 April 2018.
212. New York City Office of the Mayor (2018) 'Mayor de Blasio Appoints Laura Negrón as Chief Privacy Officer' [online]. New York: City of New York. Available from: <http://www1.nyc.gov/office-of-the-mayor/news/167-18/mayor-de-blasio-appoints-laura-negr-n-chief-privacy-officer> [Accessed 13th June 2018].
213. New York City Office of the Mayor (2018) 'Mayor de Blasio Appoints Laura Negrón as Chief Privacy Officer' [online]. New York: City of New York. Available from: <http://www1.nyc.gov/office-of-the-mayor/news/167-18/mayor-de-blasio-appoints-laura-negr-n-chief-privacy-officer> [Accessed 13th June 2018].
214. New York City Office of the Mayor (2018) 'Mayor de Blasio Appoints Laura Negrón as Chief Privacy Officer' [online]. New York: City of New York. Available from: <http://www1.nyc.gov/office-of-the-mayor/news/167-18/mayor-de-blasio-appoints-laura-negr-n-chief-privacy-officer> [Accessed 13th June 2018].
215. New York City Mayor's Office of the Chief Technology Officer (n.d.) 'IoT Guidelines' [online]. New York: The City of New York. Available from: <https://iot.cityofnewyork.us/> [Accessed 13th June 2018]
216. Edwards, L. (2016) Privacy, security and data protection in smart cities: a critical EU law perspective. 'European Data Protection Law Review.' 2 (1), pp. 28-58.
217. New York City Mayor's Office of the Chief Technology Officer (n.d.) 'FAQ - IoT Guidelines' [online]. New York: The City of New York. Available from: <https://iot.cityofnewyork.us/faq/> [Accessed 13th June 2018]
218. NYC Innovation & Emerging Technologies Workgroup (2016) 'NYC Innovation & Emerging Technologies Workgroup Presents: NYC Guidelines for the Internet of Things.' PowerPoint Slide Deck, The New York State Forum. Available from https://www.nysforum.org/events/9_14_2016/9_14_16_NYCGuidelinesIoT.pdf [Accessed 13th June 2018].
219. New York City Mayor's Office of the Chief Technology Officer (n.d.) 'IoT Guidelines' [online]. New York: The City of New York. Available from: <https://iot.cityofnewyork.us/> [Accessed 13th June 2018]
220. NYC Innovation & Emerging Technologies Workgroup (2016) 'NYC Innovation & Emerging Technologies Workgroup Presents: NYC Guidelines for the Internet of Things.' PowerPoint Slide Deck, The New York State Forum. Available from https://www.nysforum.org/events/9_14_2016/9_14_16_NYCGuidelinesIoT.pdf [Accessed 13th June 2018].
221. NYC Innovation & Emerging Technologies Workgroup (2016) 'NYC Innovation & Emerging Technologies Workgroup Presents: NYC Guidelines for the Internet of Things.' PowerPoint Slide Deck, The New York State Forum. Available from https://www.nysforum.org/events/9_14_2016/9_14_16_NYCGuidelinesIoT.pdf [Accessed 13th June 2018].
222. New York City Mayor's Office of the Chief Technology Officer (n.d.) 'FAQ - IoT Guidelines' [online]. New York: The City of New York. Available from: <https://iot.cityofnewyork.us/faq/> [Accessed 13th June 2018]
223. Angwin, J., Larson, J., Mattu, S. and Kirchner, L. (2016) Machine Bias [online]. 'ProPublica.' 23 May. Available from: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> [Accessed 14th June 2018].
224. Flores, A.W., Bechtel, K. and Lowenkamp, C.T. (2016) False Positives, False Negatives, and False Analyses: A Rejoinder to "Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And it's Biased Against Blacks." 'Federal Probation.' 80(2).
225. Cited in Powles, J. (2017) New York City's Bold, Flawed Attempt to Make Algorithms Accountable New Yorker [online]. 'The New Yorker.' 20 December. Available from: <https://www.newyorker.com/tech/elements/new-york-citys-bold-flawed-attempt-to-make-algorithms-accountable> [Accessed 19th June 2018].
226. Interview with Zachary Hecht, 27 March 2018.
227. Interview with Zachary Hecht, 27 March 2018.
228. Interview with Zachary Hecht, 27 March 2018.
229. Interview with Zachary Hecht, 27 March 2018.
230. Interview with Zachary Hecht, 27 March 2018; Zima, E. (2018) Could New York City's AI Transparency Bill be a Model for the Country? [online]. 'Government Technology.' 4 January. Available from: <http://www.govtech.com/Could-New-York-Citys-AI-Transparency-Bill-Be-a-Model-for-the-Country.html?flipboard=yes> [Accessed 14th June 2018]; New York City Office of the Mayor (2018) 'Mayor de Blasio Announces First-In-Nation Task Force to Examine Automated Decision Systems Used by the City' [online]. New York: City of New York. Available from: <http://www1.nyc.gov/office-of-the-mayor/news/251-18/mayor-de-blasio-first-in-nation-task-force-examine-automated-decision-systems-used-by> [Accessed 14th June 2018].
231. New York City Office of the Mayor (2018) 'Mayor de Blasio Announces First-In-Nation Task Force to Examine Automated Decision Systems Used by the City' [online]. New York: City of New York. Available from: <http://www1.nyc.gov/office-of-the-mayor/news/251-18/mayor-de-blasio-first-in-nation-task-force-examine-automated-decision-systems-used-by> [Accessed 14th June 2018].
232. Interview with Zachary Hecht, 27 March 2018.
233. Powles, J. (2017) New York City's Bold, Flawed Attempt to Make Algorithms Accountable New Yorker [online]. 'The New Yorker.' 20 December. Available from: <https://www.newyorker.com/tech/elements/new-york-citys-bold-flawed-attempt-to-make-algorithms-accountable> [Accessed 19th June 2018]; Interview with Zachary Hecht, 27 March 2018.
234. Interview with Zachary Hecht, 27 March 2018.
235. Interview with Zachary Hecht, 27 March 2018.

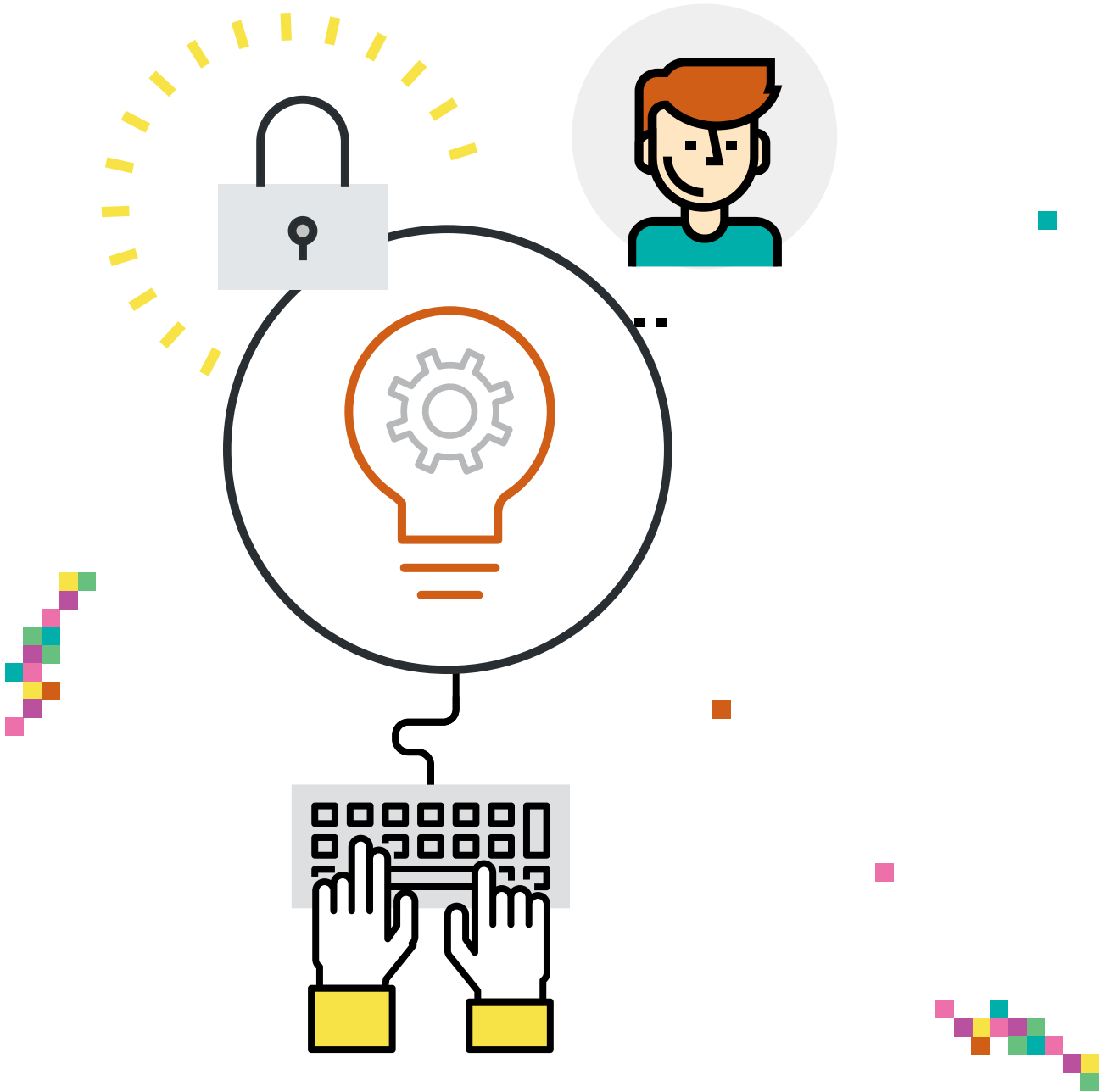
236. Powles, J. (2017) New York City's Bold, Flawed Attempt to Make Algorithms Accountable New Yorker [online]. 'The New Yorker.' 20 December. Available from: <https://www.newyorker.com/tech/elements/new-york-citys-bold-flawed-attempt-to-make-algorithms-accountable> [Accessed 19th June 2018]; Interview with Zachary Hecht, 27 March 2018.
237. Interview with Zachary Hecht, 27 March 2018.
238. Kiley, B. and Fikse-Verkerk, M. (2013) You are a Rogue Device [online]. 'The Stranger.' 6 November. Available from: <https://www.thestranger.com/seattle/you-are-a-rogue-device/Content?oid=18143845> [Accessed 13th June 2018].
239. Kiley, B. and Fikse-Verkerk, M. (2013) You are a Rogue Device [online]. 'The Stranger.' 6 November. Available from: <https://www.thestranger.com/seattle/you-are-a-rogue-device/Content?oid=18143845> [Accessed 13th June 2018].
240. Quaintance, Z. (2018) Seattle Pushes Forward as Data Privacy Leader [online]. 'Government Technology.' 6 February. Available from: <http://www.govtech.com/data/Seattle-Pushes-Forward-as-Data-Privacy-Leader.html> [Accessed 13th June 2018]; Future of Privacy Forum (2018) 'City of Seattle Open Data Risk Assessment: Final Report.' Washington, DC: Future of Privacy Forum. Available from: <https://fpf.org/wp-content/uploads/2018/01/FPF-Open-Data-Risk-Assessment-for-City-of-Seattle.pdf> [Accessed 13th June 2018].
241. Seattle Information Technology (2018) 'About the Privacy Program' [online]. Seattle: City of Seattle. Available from: <https://www.seattle.gov/tech/initiatives/privacy/about-the-privacy-program#scope> [Accessed 13th June 2018].
242. City of Seattle (2015) 'City of Seattle Privacy Principles' [online]. Seattle: City of Seattle. Available from: <https://www.seattle.gov/Documents/Departments/InformationTechnology/City-of-Seattle-Privacy-Principles-FINAL.pdf> [Accessed 13th June 2018].
243. Seattle Information Technology (2018) 'About the Privacy Program' [online]. Seattle: City of Seattle. Available from: <https://www.seattle.gov/tech/initiatives/privacy/about-the-privacy-program#scope> [Accessed 13th June 2018].
244. City of Seattle (2016) 'Privacy Policy' [online]. Seattle: City of Seattle. Available from: <https://www.seattle.gov/Documents/Departments/InformationTechnology/privacy/PrivacyPolicyFINAL.pdf> [Accessed 14th June 2018].
245. City of Seattle (2016) 'Privacy Policy' [online]. Seattle: City of Seattle. Available from: <https://www.seattle.gov/Documents/Departments/InformationTechnology/privacy/PrivacyPolicyFINAL.pdf> [Accessed 14th June 2018].
246. City of Seattle (2016) 'Privacy Policy' [online]. Seattle: City of Seattle. Available from: <https://www.seattle.gov/Documents/Departments/InformationTechnology/privacy/PrivacyPolicyFINAL.pdf> [Accessed 14th June 2018].
247. Seattle Information Technology (2018) 'About the Surveillance Ordinance' [online]. Seattle: City of Seattle. Available from: <https://www.seattle.gov/tech/initiatives/privacy/surveillance-technologies/about-surveillance-ordinance> [Accessed 13th June 2018].
248. Seattle Information Technology (2018) 'Surveillance Technologies' [online]. Seattle: City of Seattle. Available from: <https://www.seattle.gov/tech/initiatives/privacy/surveillance-technologies> [Accessed 14th June 2018].
249. Buttar, S. (2017) 'West Coast Jurisdictions Advance Community Oversight of Police Surveillance' [online]. San Francisco: Electronic Frontier Foundation. Available from: <https://www.eff.org/deeplinks/2017/08/west-coast-jurisdictions-advance-community-oversight-police-surveillance> [Accessed 14th June 2018].
250. City of Seattle (2016) 'Open Data Policy V1.0' [online]. Seattle: City of Seattle. Available from: <http://www.seattle.gov/Documents/Departments/SeattleGovPortals/CityServices/OpenDataPolicyV1.pdf> [Accessed 13th June 2018].
251. City of Seattle (2018) 'Open Data Program' [online]. Seattle: City of Seattle. Available from: <https://data.seattle.gov/stories/s/urux-ir64> [Accessed 13th June 2018].
252. City of Seattle (2016) 'Open Data Policy V1.0' [online]. Seattle: City of Seattle. Available from: <http://www.seattle.gov/Documents/Departments/SeattleGovPortals/CityServices/OpenDataPolicyV1.pdf> [Accessed 13th June 2018].
253. Murray, E.B. (2016) 'Executive Order 2016-01' [online]. Seattle: Office of the Mayor. Available from: <http://murray.seattle.gov/wp-content/uploads/2016/02/2.26-EO.pdf> [Accessed 13th June 2018].
254. City of Seattle (2016) 'Open Data Policy V1.0' [online]. Seattle: City of Seattle. Available from: <http://www.seattle.gov/Documents/Departments/SeattleGovPortals/CityServices/OpenDataPolicyV1.pdf> [Accessed 13th June 2018].
255. Future of Privacy Forum (2018) 'City of Seattle Open Data Risk Assessment: Final Report.' Washington, DC: Future of Privacy Forum. Available from: <https://fpf.org/wp-content/uploads/2018/01/FPF-Open-Data-Risk-Assessment-for-City-of-Seattle.pdf> [Accessed 13th June 2018].
256. Future of Privacy Forum (2018) 'City of Seattle Open Data Risk Assessment: Final Report.' Washington, DC: Future of Privacy Forum. Available from: <https://fpf.org/wp-content/uploads/2018/01/FPF-Open-Data-Risk-Assessment-for-City-of-Seattle.pdf> [Accessed 13th June 2018].
257. Golle, P. (2006) Revisiting the Uniqueness of Simple Demographics in the US Population. 'In: WPES 2006 Proceedings of the 5th ACM workshop on Privacy in electronic society.' New York: ACM.
258. Finkle, E. & DataSF (2016) 'Open Data Release Toolkit' [online]. San Francisco: DataSF. Available from: https://docs.google.com/document/d/1_K59q9ik5eEw9_-iiPCbQ8WSIGk0FovNz1uLajVHoi0/edit [Accessed 13th June 2018].

259. p.3, Finkle, E. & DataSF (2016) 'Open Data Release Toolkit' [online]. San Francisco: DataSF. Available from: https://docs.google.com/document/d/1_K59q9ik5eEw9_-iiPCbQ8WSIGk0FovNz1uLajVHoiO/edit [Accessed 13th June 2018].
260. Valenta, B. (2017) 'How San Francisco is Opening More Data with a Premium on Privacy' [online]. Cambridge, MA: Harvard Kennedy School Ash Center for Democratic Governance and Innovation. Available from: <https://datasmart.ash.harvard.edu/news/article/how-san-francisco-is-opening-more-data-with-a-premium-on-privacy-1135> [Accessed 13th June 2018].
261. Valenta, B. (2017) 'How San Francisco is Opening More Data with a Premium on Privacy' [online]. Cambridge, MA: Harvard Kennedy School Ash Center for Democratic Governance and Innovation. Available from: <https://datasmart.ash.harvard.edu/news/article/how-san-francisco-is-opening-more-data-with-a-premium-on-privacy-1135> [Accessed 13th June 2018].
262. Valenta, B. (2017) 'How San Francisco is Opening More Data with a Premium on Privacy' [online]. Cambridge, MA: Harvard Kennedy School Ash Center for Democratic Governance and Innovation. Available from: <https://datasmart.ash.harvard.edu/news/article/how-san-francisco-is-opening-more-data-with-a-premium-on-privacy-1135> [Accessed 13th June 2018].
263. Valenta, B. (2017) 'How San Francisco is Opening More Data with a Premium on Privacy' [online]. Cambridge, MA: Harvard Kennedy School Ash Center for Democratic Governance and Innovation. Available from: <https://datasmart.ash.harvard.edu/news/article/how-san-francisco-is-opening-more-data-with-a-premium-on-privacy-1135> [Accessed 13th June 2018].
264. eGovernment Switzerland (n.d.) 'Establishment of an electronic identity (E-ID) that is valid nationally and internationally' [online]. Berne, CH: Programme Office eGovernment Switzerland. Available from: <https://www.egovernment.ch/en/umsetzung/schwerpunktplan/elektronische-identitat/> [Accessed 19th June 2018].
265. eGovernment Switzerland (n.d.) 'Establishment of an electronic identity (E-ID) that is valid nationally and internationally' [online]. Berne, CH: Programme Office eGovernment Switzerland. Available from: <https://www.egovernment.ch/en/umsetzung/schwerpunktplan/elektronische-identitat/> [Accessed 19th June 2018].
266. Interview with Dolfi Mueller, 23 March 2018.
267. uPort (2017) First official registration of a Zug citizen on Ethereum [online]. 'Medium.' 15 November. Available from: <https://medium.com/uport/first-official-registration-of-a-zug-citizen-on-ethereum-3554b5c2c238> [Accessed 19th June 2018]; Cretin, A. (2018) It's 2018 -- Blockchain is on its way to Become the New Internet [online]. 'Medium.' 5 January. Available from: <https://medium.com/@andrewcretin/its-2018-blockchain-is-on-it-s-way-to-become-the-new-internet-7055ed6851ec> [Accessed 19th June 2018].
268. Offerman, A. (2018) 'Swiss City of Zug issues Ethereum blockchain-based eIDs' [online]. [s.l.]: European Commission. Available from: <https://joinup.ec.europa.eu/document/swiss-city-zug-issues-ethereum-blockchain-based-eids> [Accessed 19th June 2018].
269. Interview with Dolfi Mueller, 23 March 2018.
270. Kohlhaas, P. (2017) Zug ID: Exploring the First Publicly Verified Blockchain Identity [online]. 'Medium.' 7 December. Available from: <https://medium.com/uport/zug-id-exploring-the-first-publicly-verified-blockchain-identity-38bd0ee3702> [Accessed 19th June 2018]
271. Kohlhaas, P. (2017) Zug ID: Exploring the First Publicly Verified Blockchain Identity [online]. 'Medium.' 7 December. Available from: <https://medium.com/uport/zug-id-exploring-the-first-publicly-verified-blockchain-identity-38bd0ee3702> [Accessed 19th June 2018]
272. Interview with Dolfi Mueller, 23 March 2018.
273. Interview with Dolfi Mueller, 23 March 2018.
274. Interview with Dolfi Mueller, 23 March 2018.
275. Interview with Karl-Filip Coenegrachts, 3 May 2018.
276. Balkan, A. (2018) 'Indienet' [online]. [s.l.]: Indienet. Available from: <https://indienet.info/> [Accessed 19th June 2018]; Smart Circle (2013) 'City of Ghent: The Smart-Citizen is our Starting Point' [online]. [s.l.]: Euroforum. Available from: <https://www.smart-circle.org/smartcity/uncategorized/the-smart-citizen-is-our-starting-point/> [Accessed 19th June 2018].
277. Interview with Karl-Filip Coenegrachts, 3 May 2018.
278. Interview with Karl-Filip Coenegrachts, 3 May 2018.
279. Interview with Karl-Filip Coenegrachts, 3 May 2018.
280. Balkan, A. (2018) 'Hallo.gent' [online]. [s.l.]: Indienet. Available from: <https://indienet.info/hallo.gent/> [Accessed 19th June 2018].
281. Balkan, A. (2018) 'Indienet' [online]. [s.l.]: Indienet. Available from: <https://indienet.info/> [Accessed 19th June 2018]; Balkan, A. (2018) 'Hallo.gent' [online]. [s.l.]: Indienet. Available from: <https://indienet.info/hallo.gent/> [Accessed 19th June 2018].
282. Interview with Karl-Filip Coenegrachts, 3 May 2018; Balkan, A. (2018) 'Indienet' [online]. [s.l.]: Indienet. Available from: <https://indienet.info/> [Accessed 19th June 2018]
283. Balkan, A. (2018) 'Indienet' [online]. [s.l.]: Indienet. Available from: <https://indienet.info/> [Accessed 19th June 2018]
284. Balkan, A. (2018) 'Indienet' [online]. [s.l.]: Indienet. Available from: <https://indienet.info/> [Accessed 19th June 2018]; Balkan, A. (2018) 'Hallo.gent' [online]. [s.l.]: Indienet. Available from: <https://indienet.info/hallo.gent/> [Accessed 19th June 2018].
285. Interview with Karl-Filip Coenegrachts, 3 May 2018.
286. Interview with Karl-Filip Coenegrachts, 3 May 2018.
287. Interview with Karl-Filip Coenegrachts, 3 May 2018.

288. Culnane, C., Rubinstein, B.I.P., and Teague, V. (2017) 'Privacy Assessment of De-identified Opal Data: A report for Transport for NSW.' [s.l.]: CoRR. Available from: <https://arxiv.org/pdf/1704.08547.pdf> [Accessed 19th June 2018].
289. Transport for New South Wales is a state government agency that is responsible for transport within the city of Sydney
290. Jameel Asghar, H., Tyler, P and Kaafar, M.A. (2017) 'Differentially Private Release of Public Transport Data: The Opal Use Case.' [s.l.]: CoRR. Available from: <https://arxiv.org/pdf/1705.05957.pdf> [Accessed 19th June 2018].
291. Transport for NSW (2017) 'Small Business' Opal Data Boost' [online]. Sydney: Transport for New South Wales. Available from: <https://www.transport.nsw.gov.au/newsroom-and-events/media-releases/small-business-opal-data-boost> [Accessed 19th June 2018].
292. Green, B., Cunningham, C., Ekblaw, A. Kominers, P., Linzer, A. and Crawford, S. (2017) 'Open Data Privacy.' Cambridge, MA: Berkman Klein Center. Available from: <https://dash.harvard.edu/handle/1/30340010> [Accessed 19th June 2018].
293. Braun, T., Fung, B.C.M., Iqbal, F. and Shah, B. (2018) Security and Privacy Challenges in Smart Cities. 'Sustainable Cities and Society.' 39, pp.499-507; Greenberg, A. (2017) How one of Apple's Key Privacy Safeguards Falls Short [online]. 'Wired.' 15 September. Available from: <https://www.wired.com/story/apple-differential-privacy-shortcomings/> [Accessed 19th June 2018].
294. Culnane, C., Rubinstein, B.I.P., and Teague, V. (2017) 'Privacy Assessment of De-identified Opal Data: A report for Transport for NSW.' [s.l.]: CoRR. Available from: <https://arxiv.org/pdf/1704.08547.pdf> [Accessed 19th June 2018].
295. Transport for NSW (2017) 'Open Opal Dataset Documentation' [online]. (V.2.) Sydney: Transport for NSW. Available from: <https://opendata.transport.nsw.gov.au/sites/default/files/resources/Open%20Opal%20Data%20Documentation%20170728.pdf> [Accessed 20th June 2018].
296. Government Information (Public Access) Act No 52, 2009. Sydney: Government of New South Wales. Available from: <https://www.legislation.nsw.gov.au/acts/2009-52.pdf> [Accessed 19th June 2018].
297. See <https://opendataforum.transport.nsw.gov.au/t/insight-from-our-data-simple-analysis-using-the-open-opal-data/709> [Accessed 19th June 2018].
298. Transport for NSW (2017) 'Small Business' Opal Data Boost' [online]. Sydney: Transport for New South Wales. Available from: <https://www.transport.nsw.gov.au/newsroom-and-events/media-releases/small-business-opal-data-boost> [Accessed 19th June 2018].
299. Culnane, C., Rubinstein, B.I.P., and Teague, V. (2017) 'Privacy Assessment of De-identified Opal Data: A report for Transport for NSW.' [s.l.]: CoRR. Available from: <https://arxiv.org/pdf/1704.08547.pdf> [Accessed 19th June 2018].
300. Culnane, C., Rubinstein, B.I.P., and Teague, V. (2017) 'Privacy Assessment of De-identified Opal Data: A report for Transport for NSW.' [s.l.]: CoRR. Available from: <https://arxiv.org/pdf/1704.08547.pdf> [Accessed 19th June 2018].
301. Culnane, C., Rubinstein, B.I.P., and Teague, V. (2017) 'Privacy Assessment of De-identified Opal Data: A report for Transport for NSW.' [s.l.]: CoRR. Available from: <https://arxiv.org/pdf/1704.08547.pdf> [Accessed 19th June 2018].
302. Culnane, C., Rubinstein, B.I.P., and Teague, V. (2017) 'Privacy Assessment of De-identified Opal Data: A report for Transport for NSW.' [s.l.]: CoRR. Available from: <https://arxiv.org/pdf/1704.08547.pdf> [Accessed 19th June 2018].
303. Culnane, C., Rubinstein, B.I.P., and Teague, V. (2017) 'Privacy Assessment of De-identified Opal Data: A report for Transport for NSW.' [s.l.]: CoRR. Available from: <https://arxiv.org/pdf/1704.08547.pdf> [Accessed 19th June 2018].
304. Marras, M. and Laniado, D. (2018) 'BarcelonaNow at "The Web Conference 2018"' [online]. London: DECODE / Nesta. Available from: <https://www.decodeproject.eu/blog/barcelonanow-%E2%80%9C-web-conference-2018%E2%80%9D> [Accessed 18th June 2018].
305. Marras, M. and Laniado, D. (2018) 'BarcelonaNow at "The Web Conference 2018"' [online]. London: DECODE / Nesta. Available from: <https://www.decodeproject.eu/blog/barcelonanow-%E2%80%9C-web-conference-2018%E2%80%9D> [Accessed 18th June 2018].
306. Marras, M. and Laniado, D. (2018) 'BarcelonaNow at "The Web Conference 2018"' [online]. London: DECODE / Nesta. Available from: <https://www.decodeproject.eu/blog/barcelonanow-%E2%80%9C-web-conference-2018%E2%80%9D> [Accessed 18th June 2018].
307. Marras, M. and Laniado, D. (2018) 'BarcelonaNow at "The Web Conference 2018"' [online]. London: DECODE / Nesta. Available from: <https://www.decodeproject.eu/blog/barcelonanow-%E2%80%9C-web-conference-2018%E2%80%9D> [Accessed 18th June 2018].
308. Making Sense (n.d.) 'Plaza del Sol' [online]. [s.l.]: Making Sense. Available from: <http://plazadelso.cat/> [Accessed 19th June 2018].
309. Gebeiedonline (2016) 'Gebiedonline.nl: Introduction.' Available from: https://gebiedonline.nl/engine/download/blob/gebiedsplatform/69870/2016/40/2016-10-02_Gebiedonline_IntroEng.pdf?app=gebiedsplatform&class=9096&id=242&field=69870 [Accessed 19th June 2018].
310. IAmsterdam (2018) 'Renting out your Amsterdam apartment to tourists' [online]. Amsterdam: IAmsterdam. Available from: <https://www.iamsterdam.com/en/living/everyday-essentials/housing/holiday-rentals-in-amsterdam> [Accessed 19th June 2018].



decode



58 Victoria Embankment
London EC4Y 0DS

info@decodeproject.eu

[@decodeproject](https://twitter.com/decodeproject)

www.decodeproject.eu

Nesta is a registered charity in England and Wales with company number 7706036 and charity number 1144091.
Registered as a charity in Scotland number SCO42833. Registered office: 58 Victoria Embankment, London, EC4Y 0DS.

