WHEN BILLBOARDS STARE BACK
HOW CITIES CAN RECLAIM THE DIGITAL PUBLIC SPACE

May 2022
AUTHORS

Dr Tomislav Marsic,
contributions from Katja Bego

The report reflects the views of its authors only.
It was kindly funded by the City of Amsterdam.

Report design by: Green Doe Graphic Design
mikeygreen@green-doe.com

Photography from Unsplash:
Front cover, 'Aerial view of City of London buildings' by Laura Chouette. This page and divider pages, 'Amsterdam cityscape' by Sandro Gonzalez. Back page, 'Boats and buildings in Amsterdam' by Rifad Lafir.
TABLE OF CONTENTS

FOREWORD BY THE CITIES COALITION FOR DIGITAL RIGHTS 4

1. INTRODUCTION – WHEN BILLBOARDS STARE BACK 5
   1.1 Data sharing between cities, citizens and local businesses – who gets what? 8
   1.2 Public spaces and private property: cities and their changing faces across Europe 10

2. PRIVACY IN PUBLIC SPACES 12
   2.1 The current policy context: how the GDPR handles ‘personal data’ 13
   2.2 Methodological approach 16

3. PRIVATE SENSORS IN PUBLIC SPACES 17
   3.1 Interactive advertising 19
   3.2 Automatic number plate recognition 21
   3.3 WiFi tracking 22
   3.4 Cities increasingly need to act as enforcers, but still lack important resources 23

4. SMART CITIES CENSOR THE SENSORS: NEW IDEAS ON A DIFFICULT TOPIC 24
   4.1 Scandals and press reporting are important drivers 25
   4.2 Using municipal permissions as leverage for privacy 26
   4.3 Introducing a notification obligation for new sensors 28
   4.4 Developing specified DPIAs 29
   4.5 Some cities react as European and national regulations prove to be toothless 29

5. RECOMMENDATIONS: WHAT ELSE CAN CITIES DO TO PROTECT THEIR CITIZENS' PRIVACY? 30
   5.1 Use your powers – smartly! 31
   5.2 Engage the public and civil society, bring in companies 31
   5.3 Integrate privacy as a cross-sectional goal 32
   5.4 Push for better enforcement and implementation 33

6. SUMMARY 34

LITERATURE 36
FOREWORD BY THE CITIES COALITION FOR DIGITAL RIGHTS

The Cities Coalition for Digital Rights, launched by the Cities of Amsterdam, Barcelona and New York in November 2018 and now with a membership of over 50 cities worldwide, is a network of cities helping each other in the greenfield of digital rights based policymaking. The Coalition is committed to promoting and defending digital rights in an urban context through city action, in order to resolve common digital challenges and work towards legal, ethical and operational frameworks to advance human rights in digital environments.

The Cities Coalition for Digital Rights brings together cities committed to harnessing technology to improve the lives of people and communities by providing trustworthy and secure digital services and infrastructure. Local governments, working with non-governmental and civil society organisations, academia and the private sector, have an important role to play in the development of proactive and holistic policies and regulations to ensure that technology is used to increase freedom, security and privacy and that the benefits of digital technology are experienced by all.

Joint city action in networks like the Cities Coalition for Digital Rights is key for leveraging existing municipal capacities to govern the challenges that digital technologies bring about. Among these challenges is one that inspired this report: the deployment of sensors and personal data-collecting devices by companies in physical public and semi-private spaces, which undermines the right to privacy and endangers public trust.

Cities often lack the knowledge about what sensors are being deployed or do not have the competencies or capacity to address the privacy concerns they bring about. However, as the best practices gathered in this report show, municipalities are leading the way and coming up with innovative approaches, regulations, policies and principles to bind and limit the deployment of data-collecting sensors in public or semi-private spaces, and ensure people’s fundamental rights are not undermined.
INTRODUCTION – WHEN BILLBOARDS STARE BACK
Digitalising and automating processes can certainly help conserve resources, save time and increase convenience in everyday life. Examples include smart traffic systems that reduce congestion and increase the reach of public transport, pollution monitoring, street light optimisation, and the improvement of municipal services. But in addition to public actors, more and more commercial players have discovered the use of measuring the public’s interaction with advertisements, or using personal data to offer convenient services such as public parking. Where such “renegade” sensors are installed by commercial actors without making sure citizens can properly consent, we become unwitting objects of pervasive privacy infringements that we don’t have the chance to opt out from.

This does not only pose a potential violation of a basic human right, but can also damage trust in public representation as there is very little accountability regarding private monitoring in public space. As things stand, there are no formal procedures cities can follow to alleviate these problems, as they neither have a say about such practices nor sometimes even know about them in the first place.

For this report we have interviewed a number of smart city representatives from all over Europe to learn about their approaches and experiences in dealing with this and similar problems. While we have learned about intelligent and proactive countermeasures, it also needs to be said that many smart city leaders are not yet aware of these potential privacy risks to their citizens. As became clear during our conversations, there is primarily a reporting problem, resulting in cities not knowing about commercial sensors in privately owned but publicly used spaces. As a result, most cities are not only not aware of the pervasive nature of commercial sensors in city spaces, but also lack the appropriate tools to properly regulate them.

As this report also shows, however, this is about to change. As the preservation of privacy, a cross-sectional goal and tantamount to a human right, slowly sinks in, those cities most affected have taken first steps to deal with this ever-growing problem and one important goal is to share these experiences and make them widely available.

To shed some light on this little-known problem, this report seeks to showcase examples of how commercial sensors are used in city spaces, what
those cities affected have been able to do about it, and what other cities could take away from such experiences. Rapid developments in the technological sphere and significant investments in digitalisation mean we are seeing the deployment of new and sometimes experimental technology in public spaces, which necessitate a response on the local level because it is there such sensors are mounted. Gathered from a number of interviews with digital leaders and high-level representatives such as Chief Digital Officers, Chief Privacy Officers, and Data Protection Officers from leading smart cities in Europe, this report lays out how cities can step in and fill the regulatory void that technological progress has created over the past years.

The key focus of this report is publicly used spaces in private ownership, also known by the abbreviation ‘POPS’ (see section 1.2). We make this distinction because it has repercussions on how well the EU General Data Protection Regulation (GDPR) regulation is realistically being followed, given that there is an enforcement gap in the private sector (see section 2.1). In other words: cities are by design left out of the information chain where privately owned sensors have to be reported. A necessary caveat is that we are concerned with privately owned sensors inasmuch as they are commercial. What we recognize but do not address here are individual-level sensors such as doorbell video cameras or other ‘always on’ devices such as smartphones or smart watches.

Seeking answers to these problems opens new and important questions about what kind of role local decision-makers can play in ensuring the privacy and digital rights are preserved. We will explore the current priorities and challenges cities face when it comes to protecting the digital rights of their residents and explore pathways local decision-makers have at their disposal, both in regulatory and practical domains. This report seeks to help cities stay at pace with, or ahead of, such developments, rather than just reacting to them.

The privacy risks of commercial actors offering data-based services in physical city spaces have been, to some extent, discussed, though such discussions took place mostly in the context of big-tech companies such as Alphabet, Airbnb and Uber (Sadowski, 2018). There are also numerous reports on the privacy aspects of smart city services such as improving traffic flows and limiting cities’ impacts on the environment. Not much, if anything, has to our knowledge yet been said about privacy-related questions emerging from companies using publicly accessible spaces to mount their sensors. This report seeks to change this by raising awareness, offering a first assessment of the problem, and suggesting potential courses of action to cities which see themselves confronted with such developments.
1.1 Data sharing between cities, citizens and local businesses – who gets what?

In the light of megatrends such as continued urbanisation, aggravating climate emergency, and accelerated digitalisation through COVID-19, cities are increasingly forced to resort to digitalisation and automation to manage these fundamental change processes. Proliferating digital services, offered in-house or acquired on the market, have the potential to make the best use of scant financial and human resources cities have at their disposal, but at the same time pose difficult questions as to how residents retain privacy considering the ever-growing data on them. As stakes are high and time scarce, there is not much of a discussion about whether cities should play an important role in protecting their citizens’ privacy but rather how they can go about it. In this, high quality data is the foundation for good and effective governance. Digitising and automating processes can help conserve resources, save time and increase convenience of everyday life.

More than mere convenience, data-based process automation can help both citizens and cities save energy and thus confront climate change. According to data from the United Nations Development Programme, cities account for 70 per cent of the world’s greenhouse gas emissions, while city population is expected to rise from 54 per cent in 2015 to 66 per cent in 2050. This means that per capita CO₂ emissions will have to decrease rapidly in a rather short amount of time. It is therefore not surprising that cities seek to introduce smart urban transport and traffic networks to reduce traffic congestion and environmental sensors to identify potential for emissions reduction.
Cities often do not have this expertise in-house, and rely on commercial data providers to supply them with the desired infrastructure. While this arrangement helps local governments quickly acquire the desired data, it creates a certain risk as large amounts of social data come under the purview of private companies that are naturally incentivized by the profit principle rather than societal goals. This represents a classic conflict of goals, where competing ecological, economic and societal targets need to be harmonised.

Where the interplay between those targets creates misguided incentives, the results can have serious repercussions on citizens’ rights – and quickly backfire for city administrations who are increasingly grappling with outcries from civil society. One doesn’t have to resort to Black Mirror style dystopian visions to picture how even otherwise rather mundane information can threaten privacy. Even more secular data collection, such as environmental surveillance through CO₂ sensors in buildings, can reveal the number of people in a room and have thus a privacy-relevant quality. Automatic number plate recognition (ANPR) not only provides automated access to restricted parking areas or informs about traffic misdemeanours but could, in cases of improper pseudonymisation, be used to compile entire movement profiles.

Secondly, both small businesses and local governments usually suffer capacity problems and are therefore often under-equipped to properly address complex privacy concerns. Consequently, they often have limited ability to create or comply with complex regulations, lacking the legal firepower bigger players have at their disposal. Maintaining the appropriate infrastructure can be straining, especially as dangers from insecure IT can be severe. Uploading, processing and storing of data are critical points for cyberattacks. Smart grids and internet connected devices in general carry inherent vulnerabilities for data security, as well as manipulation of digital services.

“Where citizens feel exposed, they will be reluctant to make use of smart city offers. Several studies show that there is a clear connection between citizens’ perceived privacy and security in smart cities environments, and their trust towards and adoption of such services.” (Cilliers and Flowerday, 2014; van Zoonen, 2016).

Of critical importance for the successful adoption of these technologies is therefore a sound policy process that takes into consideration all involved parties. Traditional approaches revolve around a top-down process with a clear dividing line, between cities as policymakers and businesses as policy takers. Technological innovation, however, is notoriously difficult to manage with approaches that assume such a one-directional and hierarchical policy process. It has been shown that collaborative approaches work better in managing complex stakeholder networks as they follow more participative models. As a result, the traditional dividing line the top-down approach posits has been blurred, as many cities lack the remit and prerogative to set effective rules to limit the automated collection of personal data in public spaces by companies.

Cities so far have fared most positively where they managed to turn this disadvantage into a virtue by fostering cooperation with local businesses. This kind of cooperation can take many forms, such as local businesses offering footfall data to cities to better cope with COVID-19, or car producers offering extensive datasets collected by their vehicles to governments. Businesses do not only play a supportive role in smart city contexts, they also often welcome clear regulation that provides standards not only for them but also for the competition. Given, however, that cities more often than not do not possess the necessary regulatory powers to enact effective legislation, this report seeks to identify areas and tools cities can use to drive change nonetheless.

While such a process is more integrative, participation of stakeholders must not come at the cost of political control. It is this control that provides a safeguard for citizens to retain their privacy, and with it their autonomy.

---

1. With the new Data Governance Act (DGA) this kind of data sharing is about to be regulated. The DGA aims to create a framework that governs the safe sharing of sensitive data held by public offices and to regulate data sharing among private actors such as individuals and private companies.
1.2. Public spaces and private property: cities and their changing faces across Europe

As we have laid out in the introduction, the focus of this report lies on public and publicly used spaces in private ownership. We make this distinction because it has repercussions on how well the GDPR, as the relevant regulation, is realistically being followed given that there is an enforcement gap in the private sector.

In liberal democracies public spaces are the physical manifestations of basic democratic rights, such as the freedom of assembly and deliberation between citizens. Since the 1960s, when New York City introduced incentive zoning, allowing real estate developers to construct higher buildings when they declared parts of the estate “publicly accessible”, the share of ‘privately owned public spaces’ (POPS), as they are called in the UK, or ‘pseudo-public spaces’ on the European continent has steadily increased (Garrett, 2017). Examples include the areas around City Hall in London, the Potsdamer Platz in Berlin, and train stations all over Europe run and owned by private companies.

Privately-owned spaces, as de jure private property but de-facto publicly used spaces nominally open to the public, have their own rules depending on the national jurisdiction. In the remainder of this section, we briefly discuss three areas in which POPS have shown to have the gravest repercussions: constitutional law, social psychology, and politics.

While the right to private property can come into conflict with basic human rights such as the freedom of assembly, this tension has in the past predominantly been resolved differently in different European countries. In Germany, for example, there is no clear precedent for either side of the argument. The Federal Constitutional Court has so far not taken the general perspective that a basic right such as the freedom of assembly could justify a claim to use the property of third parties. However, it leaves

---

2. The European Commission differentiates between privatisation of public spaces (occupation of roads and squares by cafes and restaurants), pseudo-public spaces (privately owned, publicly accessible) and genuine public spaces (European Commission, 2019, 95).
a door open to an exception to this principle if “the area is principally in public usage and, according to local conditions, there is a monopoly position of the public sector for land owned by the Treasury.” (Joite, 2011). Following this line of argument, the Constitutional Court decided in a later case that a company, owning a publicly accessible town square in the German city of Passau, could not deny the freedom of assembly in such a space (BvQ, 25/15), ruling in favour of a flash mob protest taking place on the privately owned but publicly used square next to a public pedestrian zone (Legal Tribune Online, 2015). In the UK, on the contrary, the right to property has consistently retained priority over other competing human rights, with owners’ rights of POPS upheld against freedom of assembly or freedom of movement in several cases (Perroud, 2020).

In everyday usage for citizens, it is difficult to identify POPS as privately owned since they are rarely clearly demarcated as such from publicly owned space. Where citizens do recognize spaces as privately owned, they are often subject to restricted liberties which in turn lead to more self-policing and do not allow for normal personal freedom and encounter (Garrett, 2015). This in itself has social psychological consequences for those using these places. Cities with an extreme sell-off of public city space, such as Los Angeles, have consequently been called “entrepreneurial cities” (Harvey, 1989) and POPS themselves “dead public spaces” (Sennett, 1978). The European Data Protection Board (EDPB), which can adopt binding rulings on potential infringements of the General Data Protection Regulation (GDPR), wrote in a 2019 guideline paper:

“The intensive use of video devices has an impact on citizen’s behaviour. Significant implementation of such tools in many spheres of the individuals’ life will put an additional pressure on the individual to prevent the detection of what might be perceived as anomalies.” (EDPB, 2019)

From a political point of view, privacy infringements such as CCTV diminish the collective capacity for democratic deliberation. Tracking and surveillance lead individuals to self-censor their behaviour and alter their motives when deliberating. Stahl, for instance, argues that surveillance practices where public speech is monitored “identify speakers and treat their speech as a testimony of their beliefs” (2020, 91). A particularly dystopian but unfortunately very real example comes from Hong Kong, where protesters have destroyed surveillance cameras, blinded them by spraying paint, and built human walls with umbrellas to protect the identities of those engaging in public speech. These examples highlight why, according to Stahl, privacy infringements result in a diminishment of the capacity of the public’s capacity to critically participate in collective deliberation and produce democratic legitimacy: firstly, surveillance introduces strategic action into a communicative situation and consequently severely limits a “fully communicative speech situation” as the collective liberty of the participants is constrained and, secondly, these strategic motives erode the trust necessary for open communication.

Even though GDPR, as the relevant EU-wide legislation, prescribes that private owners have the same duties in terms of privacy protections as public authorities, the former are in practice not bound by the same level of accountability and control. Elected public bodies such as local authorities are accountable to the public at elections; private companies, on the other hand, face profit-motivated efficiency pressures that can additionally intersect with shareholder interests. Private owners of publicly used spaces therefore face a specific set of incentives that usually run contrary to effective privacy protections, since large individual-level datasets are not only hard to come by but can be very lucrative commodities when analysed or sold. Additionally, given the lack of accountability and the lack of thorough control private owners of publicly used space are confronted with, there is ample evidence that sensors installed in those places are de facto not bound by the same rigour as they would be in publicly owned spaces.

---

3. This has been shown in interviews with pedestrians in Berlin in 2017 (Deutschlandfunk Nova, 2017) and a Guardian project from 2012, which aims at identifying POPS through crowd-sourcing (The Guardian, 2012).
2. PRIVACY IN PUBLIC SPACES
2. PRIVACY IN PUBLIC SPACES

2.1 The current policy context: how the GDPR handles “personal data”

With the emergence of big data and the general increasing commodification of data, new regulation has become necessary to limit the potential to profile individuals and strengthen the right to privacy which is widely deemed to be akin to a human right. The GDPR, having entered into force in May 2016, was introduced to standardise how public entities and companies providing online services process visitors’ data on their website, or the data of their registered users. The new regulations centre the rights of the individual and require companies to openly communicate why and how personal data is used. It aims to balance out commercial and public interests in harvesting large data sets and the individual’s right to privacy.

The GDPR applies to the automatic processing of personal data which are stored (or are intended to be stored) in a filing system (Articles 2 and 3). Personal data refers to “any information relating to an identified or identifiable natural person” (GDPR, Art. 4(1)). Individuals become identifiable through identifiers “such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person” (ibid).

In addition to these factors, the scope of the regulation includes all information that could lead to the identification of an individual. This also applies to data that has been pseudonymised or encrypted, as long as these processes are reversible. Under this definition, data profiles such as those collected through eye tracking or automatic number plate recognition (ANPR) are explicitly covered by the GDPR.

The GDPR has been hailed as a global landmark privacy legislation by industry associations and consumer protection organisations alike, since its mere existence signifies progress in an area that was hitherto only weakly regulated. At the same time, critics of the GDPR point out that it has “led to a boom in box-ticking but little meaningful protection of citizens.” (Hern, 2021). Central critiques of the GDPR point out seven main arguments that question:

1. The level to which the GDPR is being enforced
2. Capacity problems with national authorities
3. The uniformity with which the GDPR is applied throughout the EU and the UK
4. Pseudonymisation as a privacy protection strategy
5. The level of compliance with the GDPR in the private sector
6. “Legitimate interests” as a major loophole
7. The degree of data protection when data is sold outside of the EU.

---

4. This implies by definition that anonymous data that cannot be restored to identify the original person is not part of the scope of the GDPR.
We will briefly discuss these points in the remainder of this section.

Perhaps the most popular criticism of the GDPR calls out a lack of enforcement of the law by the national data protection authorities (DPAs) and cities alike. This has several reasons such as differently motivated and equipped DPAs, or a complicated use of the “consistency mechanism” that DPAs use to coordinate their policies. Even though some EU member states have been more proactive in issuing fines (Heine, 2021), this general lack of equal and predictable enforcement led to a restriction of the GDPR’s application to the online world in terms of the internet, as opposed to real world applications such as the aforementioned sensors in physical spaces.

Physical spaces, as far as urban infrastructure is concerned, have been largely neglected by DPAs, even though large swaths of personal data are accrued here as the remainder of this report will illustrate. This has direct repercussions for cities, which end up having to face the consequences of this deficit with an ever-increasing amount of sensors being mounted by commercial actors while simultaneously having their hands tied in a regulatory sense. Cities are not a known category in the GDPR, as they lie outside the notification chain prescribed by the law and do not possess any remit as to enforcement of the law with regard to public spaces. While cities increasingly need to act as enforcers to protect their citizens from unwanted privacy infringements, they are not only legally ill-equipped for this role, but also lack the resources and capacities to do so.

For this reason, it is for instance effectively impossible for cities to make sure that citizens can meaningfully consent to their personal data being collected by potential renegade sensors in publicly accessible spaces, not only because cities do not have the remit to enforce this, but also because they lack the resources to have their eyes everywhere at all times. Secondly, the fact that many national GDPR supervisory institutions are understaffed does not help when trying to alleviate this problem. As a result, DPAs all over the EU have developed a strong inward focus by first and foremost making sure that actions and procedures of the public bureaucracy are in congruence with the relevant legislation. This results, at least in part, in a comparative lack of resources dedicated to actively policing the implementation of the GDPR in the private sector - something that will become more apparent in more detail in later sections of this report. This lack of resources is also true for cities, as mentioned above.

A further point of criticism refers to the fact that even though EU regulations such as the GDPR are directly applicable nationally, without the need to transpose and implement them as is the case with EU directives, the GDPR does not create a completely uniform European legal space in terms of privacy. Inconsistencies in national policy application are inherent to EU regulations and are therefore also a part of the GDPR. They take shape through differing legal and bureaucratic traditions, national levels of centralisation, and resources dedicated to police compliance of the regulation. In fact, research has shown that despite the GDPR’s inherent “consistency mechanism”, where national data supervisors cooperate to harmonise their national approaches, the application of the GDPR is not consistent throughout the EU (Sloot, 2018).

Pseudonymisation also has its flaws as a data protection strategy, but constitutes a central concept in the GDPR. The consulting company Deloitte, for instance, is of the opinion that:

“Because not all personal data is exposed, it decreases the risk of abuse of the exposed data in the case of a data breach. The GDPR sets more relaxed standards for data that is pseudonymised as compared to personal data and seems to be nudging companies and organisations to use pseudonymisation as a method of securing the personal data they process.” (Vreeman, 2018)

---

5. It should be mentioned that in contrast to the GDPR’s predecessor, the 1995 European Data Protection Directive, it applies directly as a regulation and does not have to be implemented first in the member states through a patchwork of national laws. In this respect it is an improvement over its previous iteration.
How shaky the premise of such a “decreased risk” is can be illustrated by the case of a Catholic American priest who had to resign after he had been retroactively identified as a user of a dating app. Using commercially available app signal data that did not directly identify users but instead correlated a unique numerical identifier to each mobile device, the priest was identified through time stamped location data that was extracted from these openly available pseudonymised datasets (The Pillar, 2021). Even though this case does not fall under the GDPR, as it happened in the United States, datasets are constantly hacked and leaked; pseudonymised data therefore pose a danger to individuals should such identifiers find their way into the public. This problem also touches upon a lack of proper differentiation within the GDPR between low-risk and high-risk applications, resulting in the same level of data protection regardless of the type of data processing.

Even when data are properly pseudonymised and secured from public access, research has shown that, to begin with, three quarters of the analysed companies do not even formally comply with all GDPR provisions as evidenced on a large number of company websites (Müller et al., 2019). Such a large share of non-compliance suggests more of an awareness and capacity problem rather than wilful divergence. This perspective is stressed by Freitas and Mira da Silva (2018), who found in face-to-face interviews with ten industrial small and medium enterprises (SMEs) that it is often a lack of financial and human resources that is the cause of this problem.

The GDPR has also been criticised for containing a number of loopholes that in practice allow third parties such as companies to bypass its regulations. One of those loopholes is the construct of “legitimate interests”, which has been particularly controversial as it has been termed as an overly broad and flexible tool to retain and process data by third parties. Under GDPR rules, data controllers – the individuals responsible for collecting and analysing personal data – have to weigh their own interests (which include making money) against the interest of the individual whose data is to be collected (the “data subject”). They have to disclose that data are collected on grounds of legitimate interest, but do not need to disclose what interest of the data subject has been taken into account, nor how they weighted them against each other. There is no supervision over this process, and controllers have a wide leeway in collecting personal data. According to the regulation, data subjects have the right to object to the processing of their data, forcing the controller to “demonstrate compelling legitimate grounds” for their own interest (Article 21(1)), with practically no supervision of the data controller; this puts the burden of ensuring a lawful data collection on the individual. It reduces the theoretical practice of mutual balancing interests to an “opt-out” procedure, in which companies can process the data of the vast majority of its clients.

Yet with regard to commercial sensors in cities’ public spaces, citizens are often not even offered an opt-out, as the below cases suggest. Even where they do exist in the form of signs informing citizens of personal data processing when using a service such as private parking, such opt-outs often do not represent a proper choice, as citizens are frequently not in the position to act differently given the limited number of service providers in a certain area.

Lastly, another major loophole concerns the selling of data outside of the EU. Even in a case where an EU-based customer of a non-EU (for example American) company enters into a valid consent process, allowing the company to process their personal data, this company could now legally sell this data to another American company, resulting in the data
The government announced in the summer of 2021 that it seeks to amend the UK’s privacy rules in a departure from the GDPR (Hern, 2021). Losing the protection of the GDPR. This can happen because the coverage of the GDPR is limited to data in relation to the “goods and services” of the data subject (GDPR, 3(2)a) and selling data outside the EU without the data subject involved voids the GDPR’s jurisdiction. With respect to sensor data collected in physical city spaces, this means that non-European firms could legally collect data in European cities and sell it outside the EU without having to fear any kind of retribution.

In addition to the GDPR there are a number of laws in the pipeline on an EU level, the most relevant being the Artificial Intelligence Act (AIA) and the Data Governance Act (DGA). The current draft of the AIA foresees a risk-based approach with regard to potential threats posed by AI systems such as eye-tracking or facial recognition. It foresees a ban of “subliminal components individuals cannot perceive” and the “exploitation of vulnerabilities” which would, in principle, address problems created through unannounced collection of personal data similar to the cases discussed below. Moreover, the risk-based approach in dealing with AI-related threats somewhat mitigates the above mentioned criticism of the GDPR: that applications using personal data are not rated according to the level of personal data that is collected. Transparency obligations prescribing that users and citizens must always be aware that they are interacting with AI systems would, if properly executed and implemented, alleviate some of the pressures described.

The Data Governance Act (DGA), which has recently been agreed upon by the European Parliament and the European Council, sets up mechanisms which regulate the reuse of certain data. This is relevant for commercial sensors in public spaces as sharing data that have been collected already reduces the need for setting up new sensors in the public. In terms of the law’s implementation it is not yet fully clear, however, how the legislation seeks to attain the “safe” reuse of personal data and how public sector bodies could be “properly equipped” to ensure that privacy and confidentiality will be fully preserved.

2.2 Methodological approach

This report has a comparative focus through the interviews that we led with representatives of European cities. We identified interviewees in a targeted approach through organigram analysis in a number of cities, recruiting 12 interviewees from 12 cities: Amsterdam, Barcelona, Dublin, Frankfurt (Hesse), Ghent, The Hague, Helsinki, Leeds, London, Porto, Rotterdam, Vienna. Data was derived largely through face-to-face interviews and, to a lesser extent, through traditional desk research. In an early stage of the research we invited a number of digital leaders to source, discuss and discuss the prevalence of sensors in publicly available spaces.

The interviews were semi-structured, meaning we devised a questionnaire with 5 overarching themes:

I. Examples of privacy infringements in city spaces
II. Controlling for national context
III. Salience and priority
IV. Challenges in meeting these issues
V. Cities’ needs in formulating and enacting privacy policies.

For each theme we formulated a detailed catalogue of questions. Due to the explorative character of the study, however, interviewees were allowed to deviate from the questionnaire inasmuch as new insights and findings justified steering into a different direction. Moreover, given that interviewees came from different administrative backgrounds, not all questions were equally applicable to our respondents.

For the sake of comparability with the GDPR as the major piece of regulation pre-structuring the topic, we decided to exclusively look at EU countries, plus the United Kingdom, where the GDPR for now⁶ remains in force, post-Brexit, where it is still the applicable law under the Data Protection Act. For the same reason, we opted not to include American cities who have invested in interesting policy decisions and frameworks, but tend to have a much wider remit for action than their European counterparts.

---

⁶ The government announced in the summer of 2021 that it seeks to amend the UK’s privacy rules in a departure from the GDPR (Hern, 2021).
3. PRIVATE SENSORS IN PUBLIC SPACES
Smart cities have been using sensors for several years, mostly in traffic-related areas, environmental control, parking management, and during the pandemic to measure footfall data. As mass production and technological innovation leads to ever-sinking costs, companies have increased their use of sensors in physical spaces. New services based on augmented reality applications, or the virtualisation of real physical spaces ("the Metaverse"), require precise 3D data of city spaces that are costly to produce. As the internet increasingly turns into the screen on which physical cities are being rebuilt, high quality data on public spaces are in high demand. Consequently, making maps of physical space has become the business model of a sizeable number of companies. Yet with the aforementioned implementation deficit of the GDPR in the offline world, many companies do not properly comply with it or perform the self-critical assessment the EU legislation foresees for such cases, instead bending their use case to fit the legal criteria. As one interviewee put it: "Companies are making 3D maps of our city without city hall knowing it.”

Every boost in technological capability has posed and reopened its own privacy questions. Since the widespread accessibility of camera- and video-enabled tech, legal protection from privacy infringements has become harder to enforce. It is often not allowed to directly film people in publicly accessible spaces such as on streets or shopping centres, but since many people now have doorbells with cameras, this has become a virtually empty provision. When criminal incidents happen, the police ask for camera footage of shops and members of the public, and questions of privacy only come secondary.

In order to enable and empower cities to actively shape how technological progress plays out in their public spaces, we discuss here three particularly pertinent technological developments that have recently seen widespread adoption, following the maturing of the underlying technologies.
3.1. Interactive advertising

Generating feedback on advertisements allows ad producers to better target certain audiences, increase efficiency and thereby improve return on investment. Feedback is generated primarily through cameras. These are used to read spectators’ glance, faces or body movements in reaction to the exhibited ad content. Newer applications integrate photo or live video from spectators’ faces or bodies into a (moving) image or a scenery on electronic billboards. The reactions, through retina tracking or analysis of body movements, are then analysed by algorithms drawing conclusions on the reactions to the ad content. These forms of augmented reality advertisement or ‘interactive advertising’ can be found on street furniture, pedestrian lanes, in bus shelters or shopping malls and the ad-centred use of retina tracking, and facial recognition has proliferated Europe-wide and over the world. With an outdoor advertising market poised to eclipse that of newspapers (Barker, 2020) it stands to reason that such forms of feedback generating digital billboards will only increase in the future.

Digital images of faces or the retina in high resolution are the raw materials of algorithmic analysis that can identify people, tie them to places at certain times, and thus be used to produce movement profiles. There are numerous techniques that can, to varying degrees of reliability, use such footage to draw conclusions on what the EU classifies as very sensitive data, such as eye tracking data.

Eye-tracking enabled advertising had on several occasions been made use of in, among others, the Netherlands and Belgium. Billboards were put up in (underground) train stations or other spaces which once used to be publicly owned, but have been privatised in many countries in past decades. It cannot be known whether the company had filled out data protection impact assessments in which they could have argued to what extent the operating company had a special interest justifying the usage of this technology. The city administrations, among others in Ghent and Amsterdam, were neither informed nor asked for permission. No signs referenced the existence of cameras to passers-by. Only after a public outcry and media attention did the responsible company remove these billboards.
Integrating such eye-tracking capabilities into digital billboards is not particularly new. First applications are as much as fifteen years old (Skeen, 2007). This technique makes a great use case for advertisers, since it makes visible what viewers are seeing. Eye tracking "makes the subconscious gaze visible and can reproduce gaze data even if the poster was just viewed for a split second", as a company marketing this technology lays out (Eyvido, 2021).

Collecting such precise and highly valuable data comes at a price: eye tracking data can also be used to reconstruct implicit information about a person’s ‘biometric identity, gender, age, ethnicity, body weight, personality traits, drug consumption habits, emotional state, skills and abilities, fears, interests, and sexual preferences’ (Kröger, Lutz, and Müller, 2020, 226). Certain eye tracking measures may even “reveal specific cognitive processes and can be used to diagnose various physical and mental health conditions”. Even where third party actors collect just the images, such techniques can always be applied ex-post to them. Should such information regarding specific individual persons become public, it can potentially be devastating on a personal level.

A further noteworthy implementation is the proposal of an electronic billboard in Amsterdam’s pedestrian zone, which, after consultation with the City Council, was withdrawn. The billboard space was bought by a charity that helps free girls from sexual exploitation. The screen shows a video of a young girl, representing an abuse victim, sitting in a room. The camera in the billboard scans young female spectators’ faces and “deepfakes” their faces onto the girl on the screen, so that it looks like the spectator herself is the abuse victim. For this to work, the computer first has to scan the faces of spectators, which happens without obtaining any kind of agreement. The scanned image is then processed to determine whether it belongs to a female and whether that female is in the desired age bracket to fit the girl on the screen.

Other examples of this technology aim to integrate passing spectators into a (semi-) fantasy scenery that can contain popular sports teams, wild animals, or clouds with thunder and lightning. They generate excitement through gamification, but do so without giving passers-by the possibility to withhold consent, or cities the time and the space to protect their citizens from the data fallout that is, often unwittingly, generated.

These examples reveal two central issues. Firstly, this use of surveillance techniques seems to be a stretch of the guidance by the European Data Protection Board (EDPB), according to which any video surveillance represents an invasion in privacy rights, meaning that it is only allowed when there are concrete security interests on the surveiller’s side (EDPB, 2019). It seems at least questionable whether the interest of producing a more effective advertisement outweighs the protection of fundamental rights such as privacy.

Secondly, cities are not only often not notified about the installation of such sensors in publicly accessible places, but do not receive any data protection impact assessment. The Data Protection Impact Assessments (DPIAs) are legally required and have the function to record all steps undertaken to collect and process data and identify potential risks. Data controllers at operating companies who seek to work with personal data are obliged to maintain a register for each step where personal data is being processed: what data is collected, when these data are to be deleted, and the self-assessments as to the grounds (the “legitimate interest”) on which these data are collected in the first place. These registers must be presented in the event of an audit. Should companies carry out a DPIA which then shows the data processing is risky in terms of personal data protection, those companies have to contact the supervisory authority and are obliged to provide complete documentation. But this is “rarely the case”, as one interviewee from a German data protection administration admits, because companies whitewash their applications “so that they are of no risk”.

---

7. This refers to companies with ten or more employees.
In cases where DPIAs are actually filled out, they are exclusively sent to the national data protection authority and never make it to city administrations, who are kept completely in the dark about the sensors in their public spaces – and with them citizens, too. National DPAs do not share DPIAs and are, additionally, often too severely understaffed to effectively deal with such phenomena in necessary breadth. Cities therefore have no way of knowing about the sensors being mounted when it comes to privately owned publicly accessible spaces, do not get to see those DPIAs, and are not kept in the loop.

3.2. Automatic number plate recognition

Systems that scan and recognise number plates are ubiquitous and applied in several use case scenarios, by private companies all over Europe. One well known case of quasi-public automatic number plate recognition (ANPR) usage concerns congestion charge cameras and environmental zone access controls in London. The system identifies and charges drivers coming into the central city area in order to reduce traffic congestion. It operates via a camera network linked to driving licence data held by a government agency. By the same token, the ultra-low emission zone checks against high polluting vehicles coming into the city and identifies high polluting vehicles and levies a charge on them as a way of behavioural change.

These systems are run by the transport authority but contracted to Capita, a private company which runs the contracts for the congestion charge and the low emission zone (Blackwell, 2021). In other cases, where no public contracting body stands behind the private operators, the application of such technologies assumes a different quality.

Two particular use cases stand out for different reasons. Firstly, there is the example of ANPR-based private parking garages, which scan customers’ number plates to identify and verify their eligibility to use the parking spaces. Such systems are in place in almost every major European city. For this to work, cameras scan the number plates of approaching cars and compare the text-recognized registration with data in the database. When the registration matches the data in the system, access to the parking lot is granted. In order for the system to work, it needs to store the data of service subscribers. Here it should be noted that neither text recognition services nor storage may be used from US based suppliers since the Schrems II ruling from 16th July 2020 (Court of Justice of the European Union, 2020).

Secondly, there have been cases of debt collecting companies using ANPR in order to get hold of people who have, for instance, defaulted on their loans and are not responding to efforts to contact them. For this purpose, cars were fitted with camera sensors to circle entire cities and to film and process number plate data of encountered cars to identify the debtor. Such cases have been prevalent in the US (Fang, 2015), with Amsterdam being a notable example in Europe (Dreijer, 2022). The city has since banned the service, so details of the company’s ongoing approach are unclear. From a technical standpoint, it must have collected at least tens of thousands of registration images and the location of the corresponding cars, even if filters had been applied and deleted non-relevant data.

According to the GDPR, license plate data is not only personal data, but personally identifiable information (PII). PII is any data that can be used to clearly identify an individual, such as passport numbers, fingerprints, or number plates. The practice of licence plate scanning is allowable in the context of parking

---

8. The term automatic number plate recognition referred to here is most commonly used. Other abbreviations in use are ALPR (Automatic/automated license-plate recognition), AVI (Automatic vehicle identification), CPR (Car plate recognition) and LPR (Licence plate recognition).

9. In this ruling, the Court of Justice of the European Union (CJEU) maintained that the data protection level in the United States is not on par with that in the EU and that therefore the transfer of personal data of Europeans to the US (known as “privacy shield”) is unlawful.
garages provided customers are adequately notified that their registration plates will be scanned and processed through appropriate signs. In contrast to parking garages, companies indiscriminately scanning all available number plates with the intention to identify the car holder including those of uninvolved bystanders, without notification, is unlawful according to the GDPR.

In terms of lawfulness, a case could be made that if only fragments of the registration plates were scanned, this would not constitute PII. At the same time, this argument seems unlikely to be claimed, given that these techniques are usually applied to identify car holders, especially for use cases such as debt collecting. Such use cases have been rarer but certainly need to be mentioned as they are a violation of a sizeable number of citizens’ privacy. Given that, despite the clear unlawfulness of this practice, there are so far no means to stop these surveillance practices from taking place, this is a case in point that illustrates the need for attention to this field.

3.3. WiFi tracking

WiFi tracking is probably the most widespread example of how private sensors used in publicly accessible spaces can infringe on individual privacy. WiFi tracking has been around for some time, and is widely used by private and public actors. It works through wireless routers or access points, reading WiFi identification signals smartphones send out to easier connect to available wireless networks. In the process, these devices read MAC addresses – unique identifier numbers given to each networked device on the planet. Companies use this technique, for example, in and around shopping centres or other (semi-) public places.

It allows retailers, for instance, to measure how many people pass by their store, how many enter, and track their journey within the store: through WiFi tracking it is possible to create heat maps that show customer journeys based on changes in the strength of the shoppers’ signal. The selling point of WiFi tracking is that the technology requires less new hardware and infrastructural components compared to other solutions.

Smartphones send out WiFi identification signals

In terms of compliance with the GDPR, MAC addresses are personal data since they relate to “an identifiable living individual” as the definition of the EU sets out. WiFi tracking would therefore only be allowable with the consent of the tracked party, or if tracking would be necessary for the fulfilment of a contract. Given that usage is in the majority of cases limited to passers-by, WiFi tracking is only lawful under certain conditions.

Transport for London, for instance, responsible for most of the transport network in London, collects anonymised mobile data picked up by WiFi signals in the London Underground. This is, according to London’s Chief Digital Officer (CDO) Theo Blackwell, “primarily used to understand underground congestion”. Understanding congestion allows the organisation to work against it, but it also provides a good estimate as to what extent certain locations are frequented. The data is additionally used to improve advertisement pricing: ad space is priced automatically to reflect the number of passers-by. That data is anonymised and aggregated. Even though this example is about Transport for London as a public body chaired by the Mayor of London, third parties are involved because the collection and processing of WiFi signals does not happen in house. Given that the data is anonymized, however, there is no personal information identified.

In a second case, the municipality of Enschede was fined €600,000 in 2021 by the Dutch Data Protection Authority (DDPA) for tracking without data anonymisation (Autoriteit Persoonsgegevens, 2021).

10. Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data. Personal data that has been de-identified, encrypted or pseudonymised but can be used to re-identify a person remains personal data and falls within the scope of the GDPR.
In this concrete case, the city sought to use WiFi signals as footfall data to measure the crowdedness of public spaces. The devices of passers-by were given a unique code that was processed over a longer period of time and at various sensor stations, which, according to the DDPA, could be constituted as tracking. Aside from the municipality, two companies had access to the data. Even though there was no evidence that the municipality tried to actually track people, it was fined because of insufficient privacy protections: as WiFi and camera data can be combined to identify and track people all over the city, individuals could be identified.

From patterns in such data, it can also be established where individuals live and where they work, where and when they shop and where they go in their private time. From these patterns, of course, highly sensitive data can be accrued such as people’s political affiliation, their religion (when tracking regular visits to houses of worship), extramarital affairs, therapy, or rehab. It is needless to say that such data can destroy personal lives if they are published.

These examples show what could happen if private companies were under the same kind of scrutiny as public administrations are. WiFi tracking serves to showcase that cities should become more active in regulating private sensors, as it is still being widely used even though it has been established time and again that its application is in most cases unlawful.

3.4. Cities increasingly need to act as enforcers, but still lack important resources

These three examples go to show that cities are stuck in a conflict: given the proliferation of private sensors in the public space, they increasingly need to act as enforcers of the GDPR since companies will keep making use of them where it suits their needs. At the same time, though, cities lack the information, the remit, and the capacity to properly respond to this development.

Firstly, there are no European-level rules that prescribe that cities get notified when commercial actors put up sensors in POPS. Bart Rosseau, the Chief Data Officer of the city of Ghent, told us: ‘Is this a task for the police? Should we ask citizens to alert us? If they [the sensors] are well-hidden we will never know. It’s tricky and the technology is evolving faster than the regulation.’ (Rosseau, 2021). This is a problem we have encountered in interviews with most digital leaders: cities have no way of detecting unwanted sensors in publicly accessible spaces. The fact alone that there are no reports on rogue sensors itself, however, should not be seen as evidence that there are none present in city spaces. There is no proper monitoring process to systematically find and identify sensors, nor can there be.

Secondly, municipalities only have processing assignments when it comes to the GDPR, but do not have the remit to carry out implementation tasks – execution and implementation usually lie with the national or regional level. Municipal data protection officers (DPOs) can be seen as the “extensions” of the national DPAs. While the latter can ask the former to cooperate on certain issues, the former cannot issue bans for eye-tracking billboards – that would be the remit of their national level colleagues. What DPOs can do is analyse data protection aspects when they authorise the usage of public space and refuse authorisation where they see issues.

Thirdly, cities do not have the capacity (yet) to address sensors in POPS. “We already have a lot of problems identifying our own data processing, so we haven’t gotten around to the private parties who do this”, the DPO of a large European city told us. As of yet, the city capacity to address privacy and data protection is still not sufficient. In order to improve capacity, however, the same city has already taken action. It has performed a baseline study which revealed open questions, capacity problems and changes in terms of the organisation and processes that need to happen to have a better shot at getting into the driver’s seat rather than constantly reacting to developments and innovations.

This chapter portrayed use cases and implementation problems cities face with regard to commercial sensors in publicly accessible spaces. In the following chapter we take a look at what cities have done to address these barriers to action, and where and how they got creative to overcome their shortcomings in information, implementation and capacity.
4. SMART CITIES CENSOR THE SENSORS: NEW IDEAS ON A DIFFICULT TOPIC
This chapter will focus on the policy responses of cities. What kind of action can they take? Do they have tools available to meaningfully respond to these challenges? How much of that is constrained by their capacities? Do they have the necessary responsibilities vis-à-vis national governments? How does existing EU regulation mediate cities’ policy responses?

4.1. Scandals and press reporting are important drivers

One central finding in the previous chapter is that cities have no systematic way to learn about new sensors being mounted in publicly accessible spaces. So far, one of the most effective ways for cities to get reliable information were scandals picked up by the press.

In August 2019, the Financial Times published a news report detailing live facial recognition in security cameras at London’s King’s Cross, a large privately owned area with a busy underground and international train station, a college, houses, and office buildings including Google’s UK headquarters (Murgia, 2019). Simultaneously, it became public that the Canary Wharf Group, a company that owns private offices and public spaces in the London area of the same name, was in active negotiations with a security IT supplier to install facial recognition systems in the area, which prior to the pandemic was traversed by 140,000 people daily. Facial recognition technology had also been increasingly used by the South Wales and the London Metropolitan Police, both resulting in public outcry.

In reaction to these developments, South Wales Police were challenged in court, leading to a decision by the Appeal Court that the use of facial technology breaches privacy rights (The Court of Appeal, 2020). This landmark decision then set the groundwork for a decision by the Information Commissioner’s Office (ICO), the national DPA for the UK, which raised the bar to introduce facial recognition considerably. It established a multi-step system that differentiates between facial recognition technology and live facial recognition, which it defined as follows:

“It has the ability to capture the biometric data of all individuals passing within range of the camera automatically and indiscriminately. Their data is collected in real-time and potentially on a mass scale. There is often a lack of awareness, choice or control for the individual in this process. Collecting personal data, automatically collecting personal data, and collecting biometric data.” (Information Commissioner’s Office, 2021)

The ICO based its judgement on looking at six examples of live facial recognition technologies used by private bodies. All examples showed that the organisation involved did not complete the DPIAs adequately. Essentially, while there is no ban on live facial recognition technology by private providers in the UK, there is an extremely high bar for operators to make use of them. As Theo Blackwell, London’s Chief Digital Officer, puts it: “One could argue that it is so high that it is practically impossible to meet” (Blackwell, 2021).
The case shows that scandals, and subsequent reporting, are important drivers for potentially substantial systematic change. At the same time, in most cases, sensor instances in public spaces have rarely led to public outcries; most cities are therefore vulnerable to a creeping erosion of their citizens’ privacy.

In the following section we look at what else cities are doing to get on the front foot. There are no cities with extraordinary remits. Instead, there are those finding solutions by making creative use of what powers they have.

4.2. Using municipal permissions as leverage for privacy

As has become clear throughout Chapter Three, cities do not have the remit to ban or prohibit new sensors on POPS. Our interviews have shown, however, that leveraging classic existing municipal powers including licensing or giving out permissions, is a new trend that can be effective for creating binding behavioural change.

Chapters Two and Three have shown the open questions and missing remits over privately owned and publicly used space in cities, and revealed the extent to which evermore non-public space is added to cities. As a response to this development, London City Hall published the Public London Charter in October 2021, a document which sets down principles and guidance on how new public spaces (including POPS) should be operated (Public London Charter, 2021). These principles apply as a condition of planning consent for future developments by building on existing powers in the area of urban planning and urban development. Whenever developers seek to obtain permission to build in cities, they will have to sign up to the Public London Charter, which will be inserted into the condition part of planning agreements.

The Charter contains a number of principles that constitute a code of good practice in the management of new public spaces. A section on privacy and data builds on the Surveillance Commissioners’ national code of practice, the 2018 Data Protection Act, and the above-mentioned ICO. It mandates that “Data Protection Impact Assessments (DPIAs) should be shared with City Hall... so they can be published on the London Datostore to promote transparency, compliance and good practice across the city.”

This addresses one of the most crucial limitations of cities dealing with sensors in POPS. As discussed in Chapter Three, cities not only lack the remit to prescribe or mandate rules regulating sensors in publicly accessible spaces, but are also kept in the dark as they are mostly not notified about the existence of new sensors. The Public London Charter, though only regulating new developments, tackles both of these limitations of municipal policymaking by leveraging the city’s power to withhold permission to new developments on city ground. Essentially, it creates a “supercharged planning authority”, meaning a sizeable amount of the city’s power comes from the planning law used as a lever.

Theo Blackwell, London’s CDO puts it like this:

“The Public London and Emerging Technology Charters adopted by City Hall incorporate the recent opinion by the UK Information Commissioner’s Office on the use of live facial recognition technology by non-law enforcement bodies. If a private entity has a really good reason for using live facial recognition technology, then they can make that argument but must consider factors such as impact on freedom of assembly for the users in that public square. It has to argue why using such technology is justified and why a less intrusive technology was not considered.” (Blackwell, 2021)
In addition to the Public London Charter, an Emerging Tech Charter was published, a voluntary initiative containing four principles to be accommodated when developing or applying new technologies: be open, respect diversity, be trustworthy with people’s data, be sustainable.

Again, Theo Blackwell: “Now there is the Public London Charter which will be super-charged by the Information Commissioner’s Office’s decision, and there is the Emerging Tech Charter. We’ve gone from a situation where 12 months ago the rules were unclear, to a place where key questions have to be satisfied.”

Both documents were drafted by the Mayor’s office; there was a public consultation, and the Public London Charter and the Emerging Tech Charter were both developed in the open. City Hall engaged the public on the community engagement platform Talk London, and drafts were also published as editable documents so that people could add points and questions.

While this example from London is the most far-reaching and developed we have encountered in our interviews, other cities are already using similar municipal permission leverage to get commercial actors to subscribe to a set of principles. The city of Ghent, for instance, also thinks about inserting conditions about sensors on billboards into multi-year licensing schemes for advertisement real estate that is under city (as opposed to regional) management.
The City of Amsterdam has started a process that is very similar to the London example in that the Tada manifesto contains principles about the ethical use of data. In contrast to the Public London Charter, it was developed as a bottom-up project in 2017, with the collaboration of 60 organisations in the region and led by the Amsterdam Economic Board, an independent organisation consisting of CEOs, academics and government officials. The manifesto developed a number of principles that govern the usage of data which ought to be: inclusive, controlled, tailored to the people, legitimate and monitored, open and transparent, from everyone – for everyone (Tada Manifesto, 2021). After the 2018 local elections, the manifesto became part of the coalition agreement and the parties subscribed to the ethics principles outlined. Tada has since become ingrained in the local administration, its decisions, and processes. It is used as the foundation for ‘training the trainers’ schemes from across the administration, and its principles govern the tenders for new algorithmic technologies.

Tada is also at the heart of a programme Amsterdam has assigned to the Institute for Information Law at the University of Amsterdam, which explores conditions that can be added to the municipality’s policy instruments regulating the behaviour of private companies with regards to collecting sensor data. Such instruments include licensing, subsidies, concessions, or contracts with private companies. E-mobility service providers, for instance, have to fulfil certain conditions before they are allowed to run their services in the city space, having to serve commercially potentially less attractive parts of the city in order to safeguard inclusiveness from less privileged areas. Part of this programme is also a more recent development of rules formulated by the city administration on how mobility providers have to treat the data they collect and which data they have to share with City Hall.

It is important to note that leeway to add conditions to certain permits is limited. Permits, for example, which have an impact on public spaces and safety can legally only be used to add conditions that are related to the policy area the permit seeks to address. This means, in turn, that for cities not to become liable for abuse of authority, only conditions related to the regulative intent may be inserted into such authorisations. Even where this is not yet possible, applicants receive points if they fulfil conditions on privacy and data handling as part of a ‘soft’ conditionality.

The City of Porto has similar plans with regard to mobility services providers. According to Luísa Roseira, the city’s Data Protection Officer, there are ideas to introduce obligations to report statistical data to the municipality by the operators where permissions or authorisation from the latter is required (Roseira, 2021).

4.3. Introducing a notification obligation for new sensors

Since December 2021, companies and other professional actors have had to notify Amsterdam City Hall when they mount a sensor in public spaces or publicly accessible areas. The Sensors Notification Requirement Regulation states that it is prohibited to place a sensor on street furniture, publicly accessible buildings, or on moving vehicles accessible to the public without notifying the City Council at least five days in advance. The notification also needs to indicate which data will be collected and when the sensor will be removed again. If, after a grace period of six months, sensors are still placed in public spaces without a notification to the city, the sensor will be removed (after several warnings) at the cost of the owner. Location and type of sensors are published in a publicly available map. The municipality will inform citizens as well as industry organisations and large companies such as Google about the sensor register.

11 Private individuals placing sensors in public spaces are exempted from this notification obligation.
4.4. Developing specific DPIAs

In our conversations with digital leaders we got a mixed picture of DPIAs being the main tool to operationalise the GDPR. Some interviewees argued that DPIAs were not sufficiently specific in all areas, so they ended up doing more work than other actors who might interpret it in a looser fashion.

For this reason, the City of Leeds decided to create an IoT (internet of things) supplier questionnaire, which asks specific questions in relation to connectivity, the type of data collected, and what components from which provenance IoT devices contain. Stephen Blackburn, Leeds City Council’s Innovation Manager, told us: “We need to fully understand the devices that we are using before we deploy them on a large scale. To that end, the IoT supplier questionnaire provides us with more information before we make any decisions in respect to the purchase and deployment of these devices.”

While the discussion about IoT devices started several years ago, network infrastructure operators such as city governments are only now starting to act on information security aspects. From the interviews we led in the space, the practice Leeds has adopted is a unique example for how cities can go beyond national or supranational regulatory limits by creatively using the limited room for manoeuvre they have.

4.5. Some cities react as European and national regulations prove to be toothless

These examples show that there are creative ways cities can manage, and somewhat compensate for, their lack of enforcement powers. What these examples also show is that cities have to get creative, as the national level DPA had neither the resources nor the direct experience from dealing with new developments on the ground. One digital leader in a larger European city told us: “Our DPA is not in a position to sufficiently monitor developments and provide the necessary oversight. I do not think they are close enough to the ground. They can steer the conversation and they can implement, work with government to implement legislation, but again, what do you do in terms of stopping somebody from actually mounting a sensor in the streets?”

Several interviewees told us that this is also the reason that the national DPA increasingly looks to city halls when it comes to dealing with new technological developments. Some respondents reported a close cooperation of municipal DPOs with the national DPA. Moreover, there are instances where little to no legislation is forthcoming nationally, and some cities told us that national governments are approaching them because they are reacting to newer developments the national level has not yet experienced. Several interviewees thought that local government was more advanced in many questions than their national counterparts.

While national governments have the powers to pass legislation where they see fit, some respondents thought that in many instances they become active too late, and were in danger of letting technological progress happen without setting the norms to shape and govern it. This can be explained by the difficult position national governments find themselves in: they do not want to over-prescribe and regulate every possible aspect or technology, but at the same time do not want to do nothing. Cities come into a power vacuum as they can address practical aspects of applied technological change in a way that users can understand.

To put it differently, the challenge with regulating emerging technologies lies in the fact that the full scope or penetration is not yet known, meaning that any prospective regulation would have to be set at an abstract level in order to cover the full suite of activity. The challenge for cities is therefore to come up with meaningful principles that have wide application, are not too abstract as to be impractical, but not too detailed as to actually stifle genuinely good innovation.
5. RECOMMENDATIONS: WHAT ELSE CAN CITIES DO TO PROTECT THEIR CITIZENS' PRIVACY?
If one key takeaway is that awareness needs to be raised and cities activated, it also means that cities’ inactivity up until now indirectly contributes to mainstreaming and normalising sensors placed in the public with no accountability. Therefore, in this section, we make use of the insights we gained above to suggest a number of policies and practices cities and local policymakers should consider adopting. We want to address what kind of practical action cities can take and suggest realistic pathways of action that are manageable but have also shown promise to actually garner meaningful results.

5.1. Use your powers – smartly!

Perhaps the most effective tool cities can use to push the boundaries – and regulate what is not yet regulated – is to more effectively use the levers they already have at their disposal. We have seen that cities do not have remit over classical sanctions and (in GDPR terms) enforcing mechanisms: such sanctions happen after the fact and are therefore not an ideal tool to change behaviour proactively. Setting behavioural rules ex-ante, by inserting conditions for commercial actors’ access to city resources, could prove to be much more effective.

The examples from Amsterdam, London and Leeds covered in this report have shown that cities have abundant powers at their disposal in the realm of urban planning, setting economic incentives, organising traffic, and setting procurement conditions. Cities can use such powers over permits or other forms of agreements commercial actors require from municipalities. Cities can, for instance, establish conditions that need to be fulfilled before giving out permits. Such conditions could include concrete prescriptions on how to handle citizens’ data by the companies seeking such permits and what data to share with the municipality. Given that arbitrary conditions cannot be tied to permits regulating specific domains, these conditions need to be specific to the purpose of the permit.

Therefore, instead of suggesting a one-size-fits-all approach, cities should ask themselves: “what are our core powers? What are our core experiences?” and then use these powers and experiences. If one of the few powers they have is urban planning, then that could be an effective avenue to use conditionality to initiate behavioural change. In this, cities should follow a principled approach based on their experiences and goals, as discussed in the examples above.

5.2. Engage the public and civil society, bring in companies

It can be immensely helpful for cities to bring citizens and civil society on board: not only can city administration benefit from the resources these groups bring to the table, they also generate increased legitimacy when cities negotiate with companies or other commercial actors. Where smart cities generate societal trust, they also generate support for where the use of sensors is necessary.

Cities can for instance work together with activist citizens and civil society organisations to use the court system to legally dispute companies harmfully exploiting sensitive data to cooperatively tackle enforcement issues, and thus eke out more powers for municipalities. Civil society organisations such as Foxglove, an independent non-profit law firm challenging Big Tech or governmental use of personal data, use the court system to sue companies, an approach which could help cities tackle enforcement issues. Cities can also profit from private individuals taking civil action when they see their rights being violated. In European data protection law, there is a reversal of the burden of proof, meaning that companies must prove compliance with the GDPR and not vice versa. This can be an encouraging setup for individuals to take action.
Cities should also bring local stakeholders together to communicate and mediate the desired changes in behaviour. This would ideally mean that cities use the powers described above together with businesses, not against them. There is some evidence that many companies want to play a supportive role in privacy protection, and some cities emphasised to us that they wished they had better forms of cooperation with the private sector to develop regulations together.

Cities have a natural interest in good cooperation with companies, because the latter can play a supportive role in solving societal problems such as the climate emergency or city traffic. If one important goal of cities is to acquire good data about the physical public space, one cost-effective way that doesn’t require new sensors lies in cities’ cooperation with businesses. In times where technology is still in development and markets are overvalued, it is much easier and less costly to ‘recycle’ data that have already been collected. Where cities negotiate good cooperation agreements with companies bottom-up to make data reusable, installing new sensors in public spaces is not necessary.

Our interviews have also shown that a number of cities are in negotiations with large companies over data-sharing agreements. A large city in Northern Europe was offered road and traffic data from a car manufacturer, which can be used to learn more about traffic conditions and road infrastructure. The City of Amsterdam has already been using datasets from the (Alphabet-owned) mobile app Waze since early 2019 to determine where incidents, closures and other disruptions on the roads are taking place. There are plans to intensify this cooperation in order to reduce the time it takes for the traffic control centre to respond. Another example concerns the cooperation of the City of Amsterdam with the mobile services provider Felyx to acquire traffic and other societal data. Some cities have also found ways to provide a safe exchange of data with companies.

While democratic decision-making requires policymakers to listen to their constituencies and stakeholders alike, participation of commercial interests needs to remain limited to prevent them gaining too much influence in the process and adversely affect democratic legitimacy.

5.3. Integrate privacy as a cross-sectional goal

One of the challenges city administrations face is that privacy is a cross-sectional goal pursued by sectional departments such as transport, police, healthcare. All of these actors have the same questions – but all too often, they are being dealt with in silos. It therefore makes sense to integrate privacy expertise into all departments. Cities such as Rotterdam use privacy ambassadors: employees in line departments wearing an additional ‘privacy hat’. The interviews also showed that the role of privacy officers is changing as they increasingly take on the role of educators and multipliers. This has been particularly pronounced in cities like Rotterdam, where privacy officers tutor project managers on privacy issues, who themselves then become more knowledgeable.

Such a cross-sectional approach can also be helpful in increasing cooperation between city agencies which, sometimes for political reasons, can be quite fragmented. Diana Comijs, the DPO for The Hague, told us in this context: “The cooperation between the different domains is really important, so I have to work together with the Chief Data Officer and also with people who are ahead with technological development. They have to explain to me what the privacy implications of their developments may be, but the cooperation has to be very close. That has been really important from the beginning. It is a very interdisciplinary field.” (Comijs, 2021)
When devising and executing their staffing policy, cities should therefore ideally aim to bring in staff with multidisciplinary expertise. This can also mean negotiating pushbacks within line departments who naturally seek specialists with intensive, rather than extensive, skill sets. A diverse staff with varied backgrounds and cultures, ages, and political views can help create interdisciplinarity.

5.4. Push for better enforcement and implementation

One of the core points of this report is to create awareness for cities’ positions with regard to sensors in the physical public space. As things stand, most cities have no way to know whether and where private commercial actors mount sensors in POPS. Cities should therefore not only lobby for a better enforcement of the GDPR as the relevant legal basis, but also for their own inclusion into the notification chain. This would be crucial to bring the GDPR out of ‘online only’ and into the physical, offline world.

Until now, only scandals seem to generate the attention necessary to address the problem of renegade sensors in public spaces, and it is therefore questionable how effective the GDPR is beyond regulating the internet, as we have discussed at more length in 2.1. Even though there is no doubt that sensors in publicly accessible spaces are within the regulatory scope of the GDPR, the detailed operationalisation of enforcement is clearly not there yet. A ‘law in paper only’ risks not only hollowing out the specific law itself but also weakens the state’s credibility elsewhere.

GDPR enforcement issues in the public discussion focus overwhelmingly on taming big players and getting EU member countries with vested interests such as Ireland and Luxembourg in line. Perhaps because of this specific discussion, GDPR implementation has improved over the past year, at least when measured by the number of fines, which significantly increased during 2021. As a consequence, there seems to be an overreliance on imposing more hefty fines on large companies (Ikeda, 2022) while a more in-depth debate on the role cities should play in enforcing the GDPR in the offline world has not really taken off yet.

Our interviews show that this is rooted in the problem that municipalities, confronted with sensors that they are the first (and often only) ones to notice, lack the opportunity to alert DPAs, enquire as to their owner and the data they are collecting and, consequently, ban them. In order to tackle this problem, the central recommendation in this report is to include municipalities in the notification chain, in which DPIAs need to be sent to national DPAs. Every DPIA which refers to sensors in physical spaces should also go to the responsible local authority on whose ground the sensor is mounted and be published on open platforms, accessible to citizens.

For DPAs and municipalities to deal with the resulting increased workload, some of the above criticism of the GDPR needs to be addressed. This includes, first and foremost, boosting the capacity of both national DPAs and cities and municipalities. For DPAs, this would mean addressing what has been consistently reported as understaffed authorities. For cities, it would include building knowledge and accordingly building staff capacity, potentially by initially co-assigning members of the privacy team. Understaffing and a lack of capacity of controlling authorities also lies at the core of companies collecting personalised data but not filling out DPIAs, despite the formal requirement for them to do so. Cities should therefore organise nationally to collectively push their national DPAs to increase capacity in order to improve enforcement and to advocate for better dialogue of national DPAs within the GDPR cooperation mechanism. The GDPR should consequently be amended to reflect municipalities’ role in protecting citizens’ privacy in physical public spaces.

Photo: Marc-Olivier Jodoin at Unsplash

Long exposure image of city at night
6.

SUMMARY
In this report, we have set out to raise awareness of a topic which is increasingly threatening citizen’s privacy while simultaneously flying under the radar: renegade and unaccounted for sensors in publicly accessible spaces. As the report has shown, there is major uncertainty among cities and other municipal actors of the extent of unaccounted commercial sensors in publicly accessible spaces, and how to tackle a topic that is increasingly prevalent but still not much talked about in European city spaces. **Our central recommendation in this regard is to amend the GDPR to include the responsible municipalities as addressees for DPIAs relating to sensors in publicly accessible spaces.**

Sensors in public space are particularly threatening because they remain invisible to the layman’s eye. The report at hand sought to inspire imagination about what forms of data collection might take place without us realising, and how cities can use their resources to protect their citizens’ privacy from this invisible threat.

We discussed several examples of how commercial actors have already used public spaces to mount their sensors to improve advertising through measuring the interaction with passers-by, automatic number plate recognition performed by debt collecting companies, and WiFi tracking taking place in many European cities now. We argued that in light of such developments cities increasingly need to act as enforcers, but regrettably still lack important resources and remits to become effective regulators.

Based on our interviews with digital leaders we have set out three possible courses of action cities have already taken in alleviating the privacy-based repercussions of the usage of such sensors. Firstly, some cities withhold regulatory permission to commercial development projects or operating licenses where such commercial operators do not comply with conditions set by those cities to protect citizens’ privacy, make transparent their collecting of data, or use the technology they deploy to the social benefit.

Secondly, the city of Amsterdam introduced a notification system requiring commercial actors to register any sensor they wish to put up in publicly accessible spaces with the City Council, and thereby make public the position and purpose of such a sensor.

Thirdly, the city of Leeds has developed special questionnaires for suppliers of technology in order to make sure their tech cannot be used to secretly collect personal data. The takeaway is that some cities have started to react, as European and national regulations prove to be toothless.

In the final chapter we developed a number of recommendations based on the experiences above, suggesting that cities make their consent for commercial activities in their spaces conditional on such companies agreeing to make their data collection transparent and/or agreeing to data sharing arrangements with cities. We suggested that cities engage citizens and civil society to both use the latter’s resources to take to companies together, and increase their legitimacy and negotiation power when seeking solutions with the private sector.

We argued for a better integration of privacy as a cross-sectional goal into other line departments. Not least, we discussed possibilities to enhance the enforcement of the GDPR by strengthening offline enforcement by bringing on board and involving cities in the chain of notification foreseen by the GDPR.

Given that many of the cities we interviewed have no knowledge about such sensors can mean that the proliferation of renegade sensors has not yet been widespread. It can, conversely, also mean that commercial sensors are already collecting personal data without cities being aware.

In light of these results, we hope this report raises awareness, sparks discussion and perhaps leads to the action we believe is necessary to address a potentially high-risk threat to the privacy of citizens around Europe that has not yet received the attention it requires.

6. SUMMARY
LITERATURE


Dreijer, Beryl. 2022. ‘Privacy Officer at the City of Amsterdam. Video Conference Interview on 28.01.2022.’


