WHEN THE STREETLIGHTS COME ON

How “Smart Cities” are Becoming a Surveillance State

Policy Recommendations for Building Just and Equitable Smart Cities

Brie McLemore
December 2021

CITRIS AND THE BANATAO INSTITUTE | CITRIS POLICY LAB

TARAAZ
TECHNOLOGY & HUMAN RIGHTS

WHEN THE STREETLIGHTS COME ON //

How "Smart Cities" are Becoming a Surveillance State

Policy Recommendations for Building Just and Equitable Smart Cities

Brie McLemore

December 2021

Author Contact
brie.mclemore@berkeley.edu

This paper was authored as part of the Taraaz and the CITRIS Policy Lab's 2021 Technology and Human Rights fellowship program.

Executive Summary

Implementation of “smart city” technologies are gaining increasing popularity as cities throughout the country seek to improve efficiency and livability. Driven by technological innovations that utilize interconnected networks, algorithms, and AI to predict future trends and suggest interventions, these technologies often require the collection of massive amounts of data. In doing so, residents are at increased risk of surveillance and cyberattacks. Yet cities are often not transparent about the risks these technologies pose to residents. Further, many of the promises of smart city technologies, such as improved efficiency, equity, and environmental benefits, are often not realized due to the complexities of the data collected and the failure of cities to hire experienced personnel. Due to these limitations, the proposed benefits of smart cities are often lacking, yet the negative consequences of surveillance and cybersecurity attacks are prominent.

This report provides concrete recommendations grounded in critical race, feminist, and disability rights scholarships that emphasizes the importance of centering marginalized voices within smart cities. The report concludes with priority policy recommendations to better ensure transparent, accountable, and equitable use of smart city technologies, such as: meaningfully engaging community residents, hiring independent auditors, not unnecessarily retaining personal information, prioritizing the needs of marginalized communities, building “consentful tech,” and hiring knowledgeable and culturally competent staff.

Contents

01 //

INTRODUCTION

01 //

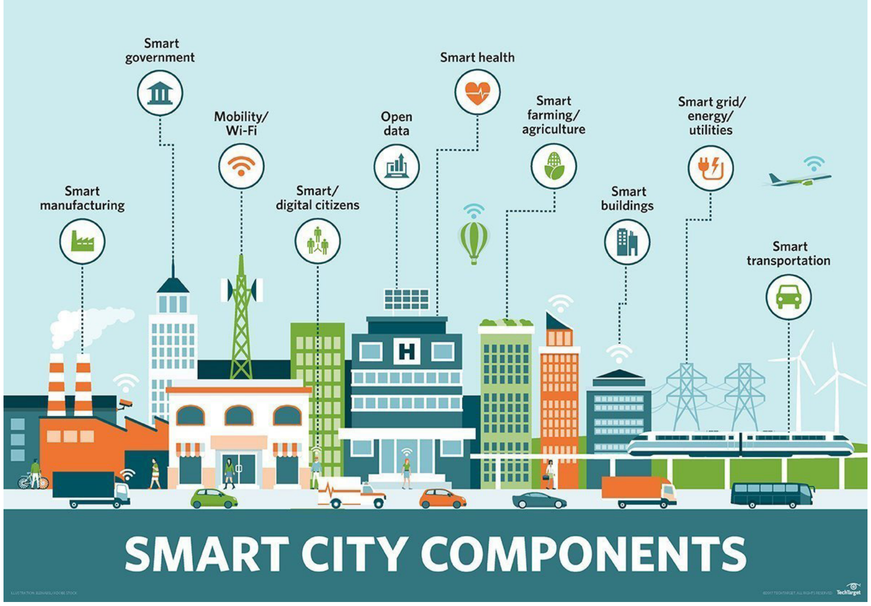
INTRODUCTION

Within the last ten years, “smart cities” have arisen as a global phenomenon that promises interconnected technologies to improve urban living and governance. Some of the technologies embedded within smart cities include smart streetlights, free city-wide wi-fi, sustainable energy sources, traffic management through artificial intelligence, smart utility meters for more efficient energy consumption, and air quality monitors. These technologies are often connected through the “Internet of Things” (IoT), which Germaine Halegoua defines as: “...a network of devices, including everyday objects and appliances (such as refrigerators, washing machines, trash cans), that are connected to the Internet, allowing people and objects as well as objects and other objects to communicate or exchange information” (Haleguoa, 2020, p. 187). This web of connected devices (e.g., sensors, lights, and meters) collects and analyzes data, which cities can then use to improve infrastructure, public utilities and increase services for residents (Business Insider, 2021).

However, while “smart” has become a key buzzword in urban planning, the concept is still largely undefined (Halegoua 2020; Sadowski and Pasquale 2015). As Sadowski and Pasquale state:

> The label is treated like a floating signifier that can change references whenever needed. Allowing for a flexible, dynamic space in which to plug a variety of products, practices, and policies. Giving them discursive cover in case they need to distance themselves if something goes wrong or doesn’t deliver on a promise” (Sadowski and Pasquale, 2015, p. 3).

In the face of such a nebulous concept, corporations have become the primary force in defining what smart cities entail, allowing them to cultivate essential products for achieving “smartness.” This vague definition is depicted in the image below, which TechTarget (2020), a leading voice in the IoT and smart city field produced. When developing their graphic to better explain what a smart city requires, the designers included essential infrastructures found in cities, such as buildings, government, transportation, and even citizens, and simply added the word “smart” to them.



Smart City Components According to the Internet of Things Agenda (TechTarget Contributors 2020)

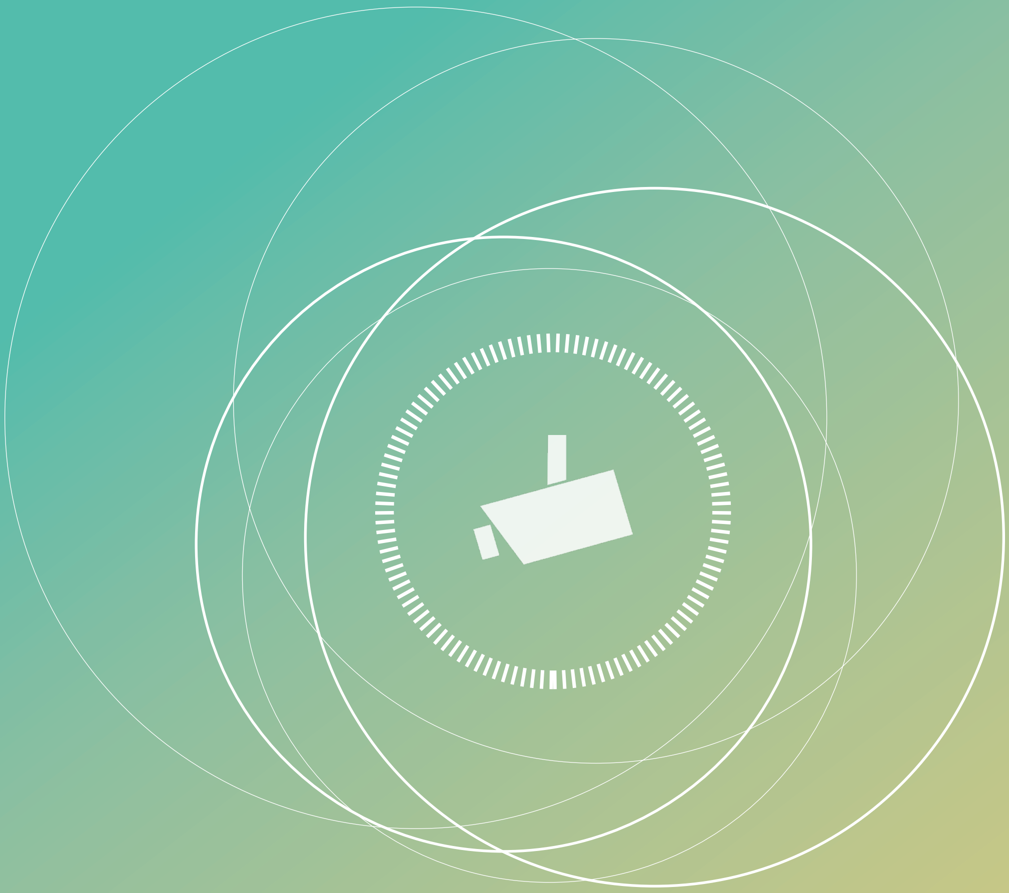
The presumed purposes of these technologies are often shaped by the disparate claims voiced in the promotional materials of competing corporations in the smart city market. But one key component is the collection of vast amounts of data as a means to interpret, as well as predict, the future trends of urban locales (Halegoua 2020, p. 5). This often includes a wide range of interconnected technologies, culminating in a vast network of digital infrastructure intended to shape, monitor, and improve every aspect of urban living. However, whether smart technologies deliver on their supposed promises is a point of contention.

San Diego’s implementation of smart streetlights serves as a prime example of the limitations of technology within the smart city. In 2015, San Diego became the first city in the United States to pilot smart streetlights. The promotional materials, provided by General Electric, as well as announcements released by city-officials, claimed that smart streetlights could track weather conditions, bike and foot traffic, and available parking to guide city planners over whether and where to implement bike paths and crosswalks, how to respond to changing weather conditions in the face of climate change, and even improve the city’s environmental footprint by directing when streetlights should be dimmed.

While these are all promising outcomes, the reality has been quite difto decrease traffic congestion, increase safety for bikers and pedestrians, or provide more public parking spaces. This is mainly because the data collected is uninterpretable and unreliable because the city did not have the foresight to hire the proper analysts needed and because the sheer amount of data was difficult to parse (Marx 2020).

Halegoua highlights how the issues facing San Diego are a common occurrence in the smart city movement. Urban planners, in a rush to acquire the designation of “smart,” quickly adopt technologies designed and marketed by corporations with little public insight. This results in the mass collection of mounting data with no clear understanding of the intended purpose. Halegoua suggests this occurrence is driven by the clever marketing of “smart” as an indicator of modernity, progress, and superiority. As she states:

> Labeling a city as ‘smart’ is a political and ideological choice. The term ‘smart city’ implies a hierarchy in which certain cities are perceived as ‘smarter’ than others and provides a general benchmark or goal for development; to attain this title, products and services can be sold and citizenry mobilized” (Halegoua, 2020, p.6).



02 //

THE PERIL OF SMART CITIES

02 //

THE PERIL OF SMART CITIES

Even if smart technologies cannot deliver on their intended benefits, they are capable of collecting vast amounts of data, which raises serious concerns for surveillance, transparency, and accountability. This occurrence is even more alarming considering the interconnected nature of urban technology. The Internet of Things (IoT) has afforded cities the ability to connect all "smart" technologies, allowing various sensors to "talk" (i.e., share data) to one another (Ranger 2020). Cities have praised this innovation for increasing efficiency, but the potential of IoT raises serious concerns, such as surveillance and cybersecurity risks.

Surveillance Risks

Smart cities often operate under the assumption that their data collection only includes "technical information," such as visual imagery and sound. These forms of data are afforded fewer privacy protections than personally identifiable information (PII), such as someone's name, address, Social Security Number, etc. This is a delineation that the city of Chicago has also adopted in regard to smart streetlights. When explicitly asked about the collection of PII through streetlight cameras, they stated: "These images will contain no sensitive PII, but some may show faces or license plate num numbers" (Array of Things 2016).

However, with the widespread adoption of technologies throughout urban locales, the distinction between technical information and PII is no longer clear-cut. When considering that smart technologies exist in conversation with one another, this creates numerous data points that can collectively provide intricate details about a person’s life. The IoT can drastically increase the amount of information obtained from just one image (Green, 2019, 93). With the widespread adoption of facial recognition software and license plate readers, it is now possible to know the name and perhaps the address of an individual from just one photo. Many smart technologies are also equipped with public wifi, which unsuspecting cell phone users might utilize without realizing how much data they are sharing.

Smart technologies often incorporate video footage, which can provide a roadmap for how a person traverses through the city. For example, video footage of one individual caught via a streetlight can tell you where this person was at a specific time. Numerous videos strung together via different streetlights have the potential to track someone across space and time, giving insight into their daily routines, places they frequent, and even people they interact with. Unfortunately, as cities rapidly adopt smart technologies without fully contending or disclosing the level of information that can be unearthed, they leave city residents vulnerable to increased surveillance with very little oversight.

Again, San Diego’s rollout of smart streetlights can serve as a cautionary tale for what is at stake in the smart city. The city’s streetlights were equipped with cameras that were constantly recording and storing data in a city-controlled database. This was done without public comment or even awareness. Then, in 2018, the San Diego Police Department (SDPD) began accessing the footage regularly. In the absence of city policies regarding the use of streetlight camera footage, the SDPD developed internal policies governing how and when it would use the data. The police department proceeded to grant itself extensive, warrantless access to video footage and integrated the data into other police technologies, such as ShotSpotters and crime mapping. Initially, the SDPD stated that it would only access footage after receiving approval from the Mayor’s office. However, the department soon decided that this process “took too long,” and instead acquired control of the footage so that it could be accessed directly (Holder 2020).

The police department did establish some limitations on the accessibility of the footage, stating that it was only to be used in response to “serious crimes.” However, SDPD refrained from defining what constitutes a “serious” crime and, having no oversight from the city, has defined the term broadly. While the footage has been used in cases involving homicide and sexual assault, it has also been used to investigate illegal dumping, vandalism, and graffiti (City of San Diego). Marx (2020) found that footage was most often accessed to surveil Black Lives Matter protests during the summer of 2020. The footage was also most likely to be pulled in low-income Black neighborhoods (ibid.).

The original promises of streetlight technology in San Diego have yet to be realized. Due to these limitations, San Diego shut off all data collection processes— except for the cameras. This has led journalists, activists, and community members to characterize smart streetlight technology as “exclusively a tool for police” (Fleming 2020). San Diego’s controversy is but one example of the heightened potential for surveillance in the smart city.

Cybersecurity Risks

The vast amounts of data collected within smart cities also make residents more vulnerable to cybersecurity threats. Smart technologies collect and store large amounts of personally identifiable information, such as addresses, social security numbers, bank account information, and even medical records. As a result, the digital networks and software smart cities require can become key targets for cyberattacks, yet cities have refrained from creating comprehensive cybersecurity protections. As smart city scholar Rob Kitchen states:

> Putting in place strong principle-led governance and management is therefore a prerequisite for creating a smart city that seeks to maximize benefits while minimizing harms. And yet, to date, there are very few documented cases of such governance and management structures being constituted. Instead, smart city initiatives have been procured and developed with little coordinated consideration of privacy and security harms and slotted into existing city management in an ad hoc fashion with minimal strategic oversight” (Kitchin 2016).

The ramifications of cybersecurity threats in smart cities have already been felt throughout the country. In February 2021, hackers gained remote access to the water plant control system in Oldsmar, Florida, and altered the amount of sodium hydroxide in the water. In March of 2018, Baltimore’s 911 automatic dispatch system was hacked, causing havoc and confusion as one of the city’s most essential services was thrown into chaos. In 2019, New Orleans had to declare a state of emergency following a cybersecurity attack in which hackers attempted to hold city-data hostage to extract ransom (Teale 2021). As more cities throughout the country attempt to become “smart,” the cybersecurity risks to residents will become more pressing than ever.

Within the last year, smart cities have gained increasing popularity due to the global Coronavirus pandemic, making questions of surveillance, transparency, and accountability even more urgent. Cities have openly and excitedly utilized cell phone data to monitor social distancing patterns and for contact tracing (White and Case, n.d.). Smart city proponents have also advocated for developing mass-video surveillance protocols to enforce social distancing measures (Shorfuzzaman et al. 2021). Cities have also increased lobbying efforts to pressure the federal government into funding smart city innovations (Crowe 2021). As this technology spreads rapidly throughout the country, cities must develop comprehensive policies to protect residents.

03 //

GUIDING PRINCIPLES

03 //

GUIDING PRINCIPLES

According to Green (2020), the architecture of smart cities is increasingly undemocratic due to power asymmetries that favor governments and corporations at the expense of city residents. Smart city technologies allow for the collection of endless amounts of data about residents' lives, fed through proprietary algorithms, which are then used to make life-altering decisions for those living within the city. This affords governments and corporations ample opportunities for surveillance and profit as the big data industry becomes more lucrative, creating a viable market for the selling of data. Due to these power inequities, Green states: "City governments eager to take advantage of new technologies must act as responsible gatekeepers and public stewards in structuring their technology to protect equity and fundamental rights" (2020, p. 92).

However, before prescribing policy suggestions for how cities can become "responsible gatekeepers," it is essential to first establish clear guiding principles and definitions for what equity, justice, and transparency entail. The Feminist Data Manifest-No (Cifor et al 2019) has created a "declaration of refusal and commitment" against the growing "harmful data regime." This manifest-no consists of thirty-two guiding principles. For this policy brief, the following are of the utmost importance:

- We **refuse** to operate under the assumption that risk and harm associated with data practices can be bounded to mean the same thing for everyone, everywhere, at every time. We **commit** to acknowledging how historical and systemic patterns of violence and exploitation produce differential vulnerabilities for communities.

- We **refuse** to understand data as disembodied and thereby dehumanized and departicularized. We **commit** to understanding data as always and variously attached to bodies; we vow to interrogate the biopolitical implications of data with a keen eye to gender, race, sexuality, class, disability, nationality, and other forms of embodied difference.

- We **refuse** any code of phony "ethics" and false proclamations of transparency that are wielded as cover, as tools of power, as forms for escape that let the people who create systems off the hook from accountability or responsibility. We **commit** to a feminist data ethics that explicitly seeks equity and demands justice by helping us understand and shift how power works.

Quoted from The Feminist Data Manifest-No

The recommendations I put forward are guided by these calls for refusal and commitments, which necessitate a critical and intersectional lens.

Another important guiding principle is a critical interrogation of "the right to privacy." While evoked by city officials, law enforcement, and residents, privacy has arisen as a critical concern but is rarely defined. In the few instances city officials have referenced privacy, it is usually done through basic refrains, such as "we value privacy" (Array of Things; City of San Diego). Smart cities that proactively develop privacy policies, no matter how vapid, are regarded as shining examples of transparency and accountability (Green, 2019). Smart city's public-facing adherence to democratic principles while simultaneously permitting surveillance can be understood as "ethics washing." According to Rob Kitchin, "ethics-washing" is a performative virtue signaling "...designed to give the impression that an issue is being taken seriously and meaningful action is occurring, when the real ambition is to avoid formal regulation and legal mechanisms" (Kitchin 2019).

This occurrence is in direct violation of the third Feminist Data Manifest-No principle outlined above, which calls for a refusal of "phony 'ethics' and false proclamations of transparency." While cities and corporations have continuously "addressed" privacy concerns, their approaches have often fallen short, raising the question of whether the "right to privacy" is a viable framework for challenging smart city surveillance. It is important to adopt a critical and historical approach to fully understand the limitations of a right to privacy to contend with the pervasive and consistently evolving technologies of smart cities. An analysis of how privacy has been filtered through the prisms of race, class, gender, and sexuality, will provide the necessary context for understanding surveillance in the smart city.

According to Toni Weller, just as surveillance has a long history predating the modern, industrial state, so do concerns for privacy (Weller 2012, 63). As state surveillance became increasingly required for benefits and services, trade-offs in privacy were consistently negotiated between the governments and their subjects (Weller 2012, p. 61). This historical privileging of privacy is evident in the modern-day, in which a claim to a right to privacy is often cited as a potential remedy to the growing surveillance apparatus. This is further evident by the rise of informational privacy as a legal framework for understanding implications for privacy in the digital age (Dubrofsky and Magnet, 2015, 4).

However, this centering of privacy should be done with an abundance of caution that affords an intersectional and historical lens. As Dubrofsky and Magnet state: “Privacy is, however, a limited lens for thinking about surveillance, since it is a right not granted equally to all” (Dubrofsky and Magnet 2015, p. 4). Any assertion of a right to privacy in the digital surveillance age requires an interrogation of the following (Dubrofsky and Magnet, 2015, p.4):

1. Who is considered to have a right to privacy?
2. Whose privacy is not a concern and why?
3. And importantly, how might a focus on these questions shape the field of surveillance studies?

As the authors state, many, such as those who are imprisoned, people receiving welfare, people with disabilities, and immigrants, have historically been denied access to privacy. Targeted surveillance of specific racial and ethnic groups not only curtails privacy but is also legitimized through the historical limitations of the privacy they have been afforded. Historically, as Igo states, “citizens viewed and wielded privacy differently depending on their status and circumstances, and some could barely access it at all” (Igo 2018, p. 9).

However, it is essential to note that while privacy has been historically denied, it has also been weaponized in the pursuit of violence. As Rachel Hall asserts, an evocation of “privacy” has traditionally allowed for patriarchal, interpersonal violence that takes place within the “privacy” of one’s home (Hall 2015, p. 127). This occurrence can trace its historical roots to the nineteenth century, in which privacy was bestowed upon men who governed their households. Citing Charlotte Perkins Gillman, Igo states that this “honoring ‘private life’ was not the same as honoring the rights of its participants, especially women and other dependents” (Igo 2018, p. 23).

This understanding of privacy has led some surveillance scholars to reject calls for increased privacy protections. According to Hall, the limitations of a right to privacy requires scholars to “shift critical surveillance studies away from matters of privacy, security, and efficiency to a consideration of the ethical problem of combating new forms of discrimination that are practiced in relation to categories of privilege, access, and risk” (Hall, 2015, p. 147).

In addition, Hall asserts that reliance upon privacy doctrine falsely universalizes the experience of surveillance as something that equally impacts all. Due to these limitations, the recommendations I put forward do not rely upon legal avenues to enact change. Instead, my recommendations are influenced by activists and scholars who adopt critical approaches to understanding surveillance. In doing so, I hope to develop comprehensive recommendations that center equity and justice instead of individualist calls for privacy.

04 //

RECOMMENDATIONS

04 //

RECOMMENDATIONS

The proposed recommendations are informed by a thorough literature review and influenced by the city of Portland's Data Privacy and Information Protection Principles and an interview I conducted with Brian Hofer, a civil rights attorney and founder of the Oakland Privacy Advisory Council (see Appendix for more details).

Recommendation 1: Meaningfully Engage Community Residents

One of the key limitations in smart cities is the ability to ensure transparency and accountability. As the city of Portland highlights, smart cities must clearly document and share how the city uses, manages, and collects data and identify who has access to said data. This could be achieved in various forums but should consider the history of disenfranchisement many community residents have experienced, which has afforded city residents' inequitable access.

Chicago can provide an important case study for analyzing city approaches to transparency and accountability. After San Diego initiated its smart streetlight program, Chicago began implementing its own smart streetlights, which has become the largest conversion project in the country.

However, unlike San Diego, Chicago’s initiative was highly publicized, provided opportunity for community input, and developed and published a comprehensive privacy policy, which was informed by the resident feedback received (Green, 2019, p. 107). These protocols were then published online for all residents to review. Due to these protocols, Chicago has been heralded as a shining example of how democratic processes and accountability can materialize within the smart city (Green 2019, p. 107).

Despite this more community-driven approach, as compared to San Diego, the city still refrained from establishing procedures or guidelines for law enforcement’s access to the data, despite urging from numerous residents and lawyers (Elahi 2017). Also, while the city held numerous open forums to discuss the smart streetlight initiative, none of these forums occurred in predominantly Black neighborhoods, even though smart streetlights were first implemented in neighborhoods throughout the South Side, which are predominately Black and low-income (Array of Things, 2016; CDOT, n.d.). Chicago provides an important example of how equity and surveillance questions should be front and center when ensuring transparency and accountability.

To ensure that smart cities are transparent and accountable to all residents, Brian Hofer suggests cities should hold community outreach meetings at every district in the city each month. City officials and privacy commissions should be in attendance to receive feedback and share the current status of smart city development. Holding these meetings frequently and throughout the city will allow for increased convenience for residents, which will result in more ample opportunities for public participation.

The Detroit Digital Justice Coalition (DDJC), which is comprised of Detroit-based activists and organizations advocating for communication as a fundamental human right, and the Detroit Community Technology Project (DCTP) released justice principles for the use and creation of technologies that are rooted in community needs. In their report, the organizations recommend engaging residents “offline” due to internet access inequities that create imbalances in transparency and accountability. As mentioned earlier, while Chicago did conduct some limited in-person meetings, the city published all protocols on the Internet, limiting who has access.

According to a survey conducted by the DDJC and DCTP, most residents acquire knowledge of technological innovations during workshops and events. Still, these can be infrequent and hard to access for many. As a remedy, cities should partner with local recreation centers, schools, and organizations that work directly with communities to spread awareness about developing smart city technologies (Detroit Digital Justice Coalition, 2017, p. 2). In addition, smart cities should also ensure that all resources are available in the various languages that reflect the demographics they serve.

Recommendation 2: Hire Independent Auditors

Both the City of Oakland and the DDJC/DCTP have advocated for independent audits of smart city initiatives, which can achieve various tasks. The DDJC/DCTP suggests that third-party security audits should be performed regularly to ensure anonymity and cybersecurity protections. One of the key aspects of smart cities is the ability for the public to access open data in the name of transparency. However, as the DDJC/DCTP points out, this can also be a source of "fear and harm to residents" since open access data can unearth identifying information about residents (i.e., location-based crime reports). As a protective measure, the organizations recommend that security audits be performed and for penetration tests to be regularly conducted to expose potential vulnerabilities that could threaten residents' anonymity (Detroit Digital Justice Coalition, 2017, p.2).

Brain Hofer also suggests hiring independent auditors that can ensure that technologies are achieving what they promised and as a protection against "mission creep." As I have mentioned, it is common for data within smart cities to be shared with other city agencies (i.e., law enforcement) and corporations tasked with implementation and their various partners. A yearly audit conducted by a third party can thoroughly investigate whether mission creep is occurring and whether this violates the city's protocols. These findings should be made publicly available online and through in-person forums (as detailed above).

Recommendation 3: Do Not Unnecessarily Retain Personal Information

In developing this recommendation, the DDJC/DCTP focused explicitly on information provided by residents when applying for access to city services (i.e., entering a license plate number at a city parking meter). To prevent unauthorized uses of such data, the Detroit coalition advocates for cities to implement provisions to not retain any personal information from these city services. One example they highlight is New York City's Municipal ID program, which did not store cardholders' personal background information. This provision was designed with equity principles in mind since those depending on these cards tend to be low-income, people of color, individuals experiencing homelessness, and undocumented immigrants (Detroit Digital Justice Coalition, 2017, p. 2).

While DDJC/DCTP focus specifically on situations where residents provide information to the city, this recommendation must be expanded upon considering the myriad ways smart cities can collect information about residents, with or without their consent or even knowledge. To account for this, I advocate for smart cities to not retain personal information for any of the data collected through sensors and nodes throughout the city. This sentiment is reflected in the city of Portland’s “data utility” principle, which states: “All information and data processes must bring value to the City of Portland and the communities the City serves. The City will collect only the minimum amount of Personal Information to fulfill a well-defined purpose and in a manner that is consistent with the context in which it will be used.” Principles such as these ensure that smart cities only collect the amount of data necessary for the tasks at hand. This will prevent smart cities from collecting unnecessary amounts of data that place residents at risk. It will also ensure that smart cities take the time to think critically about what they hope technologies will accomplish and the necessary steps for obtaining this goal.

Recommendation 4: Prioritize the Needs of Marginalized Communities

The city of Portland has also adopted an “equitable data management” principle, which prioritizes the needs of marginalized communities regarding what data is collected and what its intended uses will be. Such a policy can ensure that BIPOC, queer, disabled, immigrant, and unhoused residents are not only agents in smart city designs but that initiatives are tailored specifically for their needs.

To achieve this, cities must acquire a deep understanding of the communities they serve and their relation to city services. For example, locales serving Indigenous communities should adopt the CARE Principles outlined by the Indigenous Data Sovereignty Interest Group. The organization defines C as “Collective Benefit,” in which data planning, implementation, and evaluation processes should be in service to the needs of Indigenous communities and should strive for equitable outcomes (Research Data Alliance International Indigenous Data Sovereignty Interest Group., 2019, p.2).

Smart cities should also center the voices and needs of community members with disabilities. According to the CDC, over 70% of disabled Americans live in metropolitan counties (defined as having a population of 250,000 or more) (Zhao et al., 2016). In addition, more than 25% of people living in U.S. cities are either seniors or people living with a disability, and by 2050, it is estimated that one out of every seven city dwellers will have a disability. This occurrence is particularly concerning for smart cities, which 60% of global experts agree are inadequately meeting the needs of residents with disabilities (The Mobility Project 2019).

To be more accessible, smart cities should prioritize the needs of disabled communities and ensure that they are afforded agency and even a voice in the development of smart technologies. One key theoretical framework is that of crip-technoscience, which is a methodology for “world-building and world-dismantling practices by and with disabled people and communities that respond to intersectional systems of power, privilege, and oppression by working within and around them” (Hamrai and Fritsch, 2019, p. 4-5).

Chicago’s smart streetlight initiative provides a prime example of what prioritizing community members’ needs can look like. When determining the location of smart streetlights in Pilsen, a predominantly low-income Latinx neighborhood, the city consulted community organizations and research groups. In doing so, the city discovered that the community wanted to utilize the streetlight’s ability to track environmental conditions to document the neighborhood’s air quality due to an increase in asthma rates. The city then strategically placed the streetlights in locations that would collect the most optimal data. This data was then made open, free, and available to the public (Mitchum 2016).

However, it is essential to note that, while this was a clear beneficial outcome, these streetlights were also equipped with cameras. It is important that, when ensuring that marginalized communities are prioritized in smart city initiatives, they are also able to obtain these services without being subjected to increased surveillance as a “trade-off.”

Recommendation 5: Build “Consentful Tech”

The Allied Media Project and the Mozilla Foundation created a comprehensive zine detailing the importance for consent in digital technology. As the authors state, conversations concerning consent and our physical bodies have gained increased attention. Still, there is less conversation on the importance of consent for our digital bodies, which consists of various personal data. As in many other data spheres, data is retrieved and shared in non-consensual ways within the smart city. One crucial example offered by the zine looks at how private information such as biometric data can be shared across various databases, putting vulnerable people such as those with disabilities, immigrants, and the poor, at increased risk (Lee and Toliver, 2017, p.4).

Smart cities are plagued with issues of consent as the ability to agree or disagree with privacy policies is non-existent. This has led some technology scholars to question whether one’s right to choose what personal information they exchange disappears once they enter a smart city (Taylor 2019). As smart city scholar Lilian Edwards pointedly states: “while consumers may at least have theoretically had a chance to read the privacy policy of their Nest thermostat before signing the contract, they will have no such opportunity in any real sense when their data is collected by the smart road or smart tram they go to work on, or as they pass the smart dustbin” (cited in Taylor 2019).

Smart cities exist as a space where consent is most vital but also the most difficult to obtain. Simply opting in or out, or checking yes or no, are not efficient measures for ensuring consent. Instead, city-officials should strive to design consentful technologies, which are “applications and spaces in which consent underlies all aspects, from the way they are developed, to how data is stored and accessed, to the way interactions happen between users” (Lee and Toliver, 2017, p.6). In developing this concept, the Mozilla Foundation and Allied Media Project built off of the F.R.I.E.S. model of consent developed by Planned Parenthood which defines consent as: freely given, reversible, informed, enthusiastic, and specific (Lee and Toliver, 2017, p.8).

The community-driven challenges to Toronto’s Sidewalk Lab project gives insight into how residents can challenge proposed smart city technologies that do not provide opportunities for consent. In 2016, Google announced plans to transform the Toronto Quayside into “the most innovative district in the entire world” (Walker 2019). This project would have implemented numerous data sensors capable of monitoring every aspect of public space without any way for residents to opt-out. As tech scholar and former Sidewalk Labs consultant, Ann Cavoukian stated “The tech, the sensors are on 24/7, all the time. People don’t have an opportunity to consent, or revoke consent, to the collection of their personal data” (Johnston 2020).

Activists were able to sound the alarm of the dangers Sidewalk Labs posed and increase community engagement. Over 21,000 Toronto residents attended meetings or gave feedback on the Sidewalks Lab project, challenging the project’s disregard for their ability to consent to such high levels of data collection. Following increased pressure and backlash, the project was effectively abandoned in 2020 (Walker 2020). While this example took place in Canada, it can also provide an important blueprint for smart domestic cities. Toronto residents did not rely on legal avenues specific to the Canadian government. Instead, community members mobilized themselves by raising awareness and voicing concerns. This can provide an essential framework for how any city can challenge projects that do not rely upon “consentful tech.”

Recommendation 6: Hire Knowledgeable and Culturally Competent Staff

One issue currently facing smart cities is the limited knowledge of personnel and staff. As mentioned earlier, one of the limitations facing San Diego’s smart streetlight initiative was that the city had failed to hire staffers who could clean and interpret the data. In addition, smart city technologies have complicated data collection capabilities, which requires specific expertise. Due to this, Brian Hofer suggests that cities invest in dedicated staff members who specialize in data information and technology. These staff members should review and vet all possible technologies prior to their adoption for questions of surveillance, equity, and transparency. These staff members should also inform key city officials and stakeholders of concerns regarding these technologies so that all governing bodies can be informed when making decisions. Hired technologists can also communicate with city residents about technologies that are being considered.

Not only should these staff members be trained technologists, but they should also be culturally competent and reflect the demographics they serve. Smart city staffers should know the various customs, lived experiences, and ethics amongst and within all cultural groups within a city. This will ensure that policies and principles aren’t solely reflective of Western ideals. As mentioned earlier, it is also essential that smart city materials be produced in various languages to be accessible to all residents. This would require smart cities to hire bilingual technologists who can effectively translate complex designs and innovations for all within the smart city.

05 //

CONCLUSION

05 //

CONCLUSION

As smart cities become increasingly popular throughout the country, city officials must adopt comprehensive policies and protocols to protect residents from the increased potential for surveillance. These policies must acknowledge and account for the historical legacies that have created inequitable consequences for surveillance based on race, ethnicity, gender, sexuality, immigration status, and ability. Smart city policies should also place questions of equity and justice front and center to ensure that smart city technologies are respecting the autonomy and dignity of vulnerable residents and actually operate in service to them. I have provided a brief overview of some recommendations city planners should consider, but many other activists and scholars are working at the intersection of critical surveillance studies that cities should consult.

REFERENCES

Icons were downloaded from Flaticon and shutterstock. All images are from Wikimedia Commons, Pexels.com, and Pixabay.com.

1. Array of Things Operating Policy. (2016). https://arrayofthings.github.io/final-policies.html

2. "By the Numbers: Statistics on Disability & Cities" (2019, April 1). The Mobility Project. https://themobilityproject.com/Articles/2019/04/01/Disability-Statistics.aspx

3. CDOT. (n.d.)."Chicago Smart Lighting Program." https://chicagosmartlighting-chicago.opendata.arcgis.com/

4. Cifor, M., Garcia, P., Cowan, T.L., Rault, J., Sutherland, T., Chan, A., Rode, J., Hoffmann, A.L., Salehi, N., Nakamura, L. (2019). Feminist Data Manifest-No. Retrieved from: https://www.manifestno.com/.

5. City of San Diego. (2019). Public Meeting: Smart Streetlights. https://www.sandiego.gov/sites/default/files/sust-smartstreetlightpublicmeeting-091019.pdf

6. Crowe, C. (2021). New Lobbying Group to Advocate for Cities Amid Potential Windfall of Federal Infrastructure Dollars. SmartCities Dive. https://www.smartcitiesdive.com/news/new-lobbying-group-to-advocate-for-cities-amid-potential-windfall-of-federa/605460/

7. Detroit Digital Justice Coalition. (2017). "Recommendations for Equitable Open Data."https://github.com/datajustice/report/blob/gh-pages/downloads/DataJusticeReport.pdf

8. Dubrofsky, Rachel E., and Shoshana Amielle Magnet. (2015). "Introduction: Feminist Surveillance Studies and Critical Interventions." Feminist Surveillance Studies edited by Dubrofsky and Magnet. Duke University Press.

9. Elahi, Amina. (2017). "Array of Things Sensor Policy Leaves Law-Enforcement Question Open." Chicago Tribune. https://www.chicagotribune.com/business/blue-sky/ct-privacy-policy-array-of-things-bsi-20160819-story.html.

10. Fleming, Omari. (2020, July 20). "Data Collection Has Stopped, but Smart Streetlight Cameras Still Rolling." NBC San Diego. https://www.nbcsandiego.com/news/local/data-collection-has-stopped-but-smart-street-light-cameras-still-rolling/2369186/.

11. Green, Ben. (2019). The Smart Enough City: Putting Technology in Its Place to Reclaim Our Urban Future. MIT Press.

12. Halegoua, Germaine. (2020). Smart Cities. MIT Press.

13. Hall, Rachel. (2015). Terror and the Female Grotesque: Introducing Full-Body Scanners to U.S. Airports. In Feminist Surveillance Studies, edited by Rachel Dubrofsky and Shoshana Amielle Magnet. Chapel Hill, NC: Duke University Press.

14. Hamraie, Aimi and Kelly Fritsch. (2019).“Crip Technoscience Manifesto.” Catalyst. 5(1). https://doi.org/10.28968/cftt.v5i1.29607.

15. Holder. Sarah. (2020, August 6). “In San Diego, ‘Smart’ Streetlights Spark Surveillance Reform.” Bloomberg News. https://www.bloomberg.com/news/articles/2020-08-06/a-surveillance-standoff-over-smart-streetlights.

16. “How IoT and smart city technology works: Devices, applications and examples.” (2021, February 2). Business Insider. https://www.businessinsider.com/iot-smart-city-technology

17. Igo, Sarah E. 2018. The Known Citizen: A History of Privacy in Modern America. Harvard University Press.

18. Johnston, Ryan. (2020, May 27). “Digital privacy concerns will follow Sidewalk Labs to next venture, says former consultant.” Statescoop. https://statescoop.com/ann-cavoukian-waterfront-toronto-digital-privacy-concerns-sidewalk-labs/

19. Kitchin, Rob. (2016) Getting smarter about smart cities: Improving data privacy and data security. Data Protection Unit, Department of the Taoiseach, Dublin, Ireland.

20. Lee, Una and Toliver, Dann. (2017). Building Consentful Tech. https://www.andalsotoo.net/wp-content/uploads/2018/10/Building-Consentful-Tech-Zine-SPREADS.pdf

21. Marx, Jesse. (2020, July 2020). “Smart Streetlights Are Now Exclusively a Tool for Police.” Voices of San Diego. https://www.voiceofsandiego.org/topics/public-safety/smart-streetlights-are-now-exclusively-a-tool-for-police/.

22. Mitchum, Rob. (2016, August 29). “Urban sensing project will measure air quality, traffic, climate and more.” UChicago News. https://news.uchicago.edu/story/chicago-becomes-first-city-launch-array-things

23. Ranger, Steve. (2020 February 3). “What Is the IoT? Everything You Need to Know about the Internet of Things Right Now.” ZDNet. https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/.

24. Research Data Alliance International Indigenous Data Sovereignty Interest Group. (September 2019). “CARE Principles for Indigenous Data Governance.” The Global Indigenous Data Alliance. https://www.GIDA-global.org

25. Sadowski, Jathan, and Frank Pasquale. (2015). “The Spectrum of Control: A Social Theory of the Smart City.” First Monday, June. https://doi.org/10.5210/fm.v20i7.5903.

26. Shorfuzzaman, Mohamma, Hossain, M. Shamim, and Alhamid, Mohammed F. (2020, November 5). “Towards the sustainable development of smart cities through mass video surveillance: A response to the COVID-19 Pandemic. Sustain Cities Soc. https://dx.doi.org/10.1016%2Fj.scs.2020.102582

27. Smart City PDX. (2019, June 19). “Data Privacy and Information Protection Principles for the City of Portland.” https://static1.squarespace.com/static/5967c18bff7c50a0244ff42c/t/5d0aec446939ce00011ec049/1560996933477/COP_PIP_handout_June19_2019.pdf

28. Taylor Ben (2019, March 20). Smart Cities in North America: How can informed consent work? (Part 2). The Data Privacy Group. https://thedataprivacygroup.com/blog/2019-3-20-smart-cities-in-north-america-how-can-informed-consent-work-part-2/

29. Teale, Chris. “The smart city tech most at risk for cyberattacks: report.” Smart Cities Dive. March 26, 2021. https://www.smartcitiesdive.com/news/the-smart-city-tech-most-at-risk-for-cyberattacks-report/597365/

30. TechTarget Contributors. (2020, July 16). “What Is a Smart City? Definition from WhatIs.com.” TechTarget. https://internetofthingsagenda.techtarget.com/definition/smart-city.

31. Walker, Alissa. (2019, June 24). “Here is Sidewalk Labs’s big plan for Toronto.” Curbed. https://archive.curbed.com/2019/6/24/18715669/sidewalk-labs-toronto-alphabet-google-quayside

32. Walker, Alissa. (2020, May 7). “Sidewalk Labs’ ‘smart city’ was destined to fail.” Curbed. https://archive.curbed.com/2020/5/7/21250678/sidewalk-labs-toronto-smart-city-fail

33. Weller, Toni. (2012). “The Information State: A Historical Perspective on Surveillance.” In Routledge Handbook of Surveillance Studies. Routledge.

34. White & Case. (n.d.) 2020 Annual Review: Covid-19 could help fast-track support for smart cities.” https://www.whitecase.com/publications/insight/covid-19-could-help-fast-track-support-smart-cities

35. Zhao, Guixiang et al. (2016). Prevalence of Disability and Disability Types by Urban–Rural County Classification—U.S. American Journal of Preventive Medicine. 57 (6). p. 749 – 756

APPENDIX

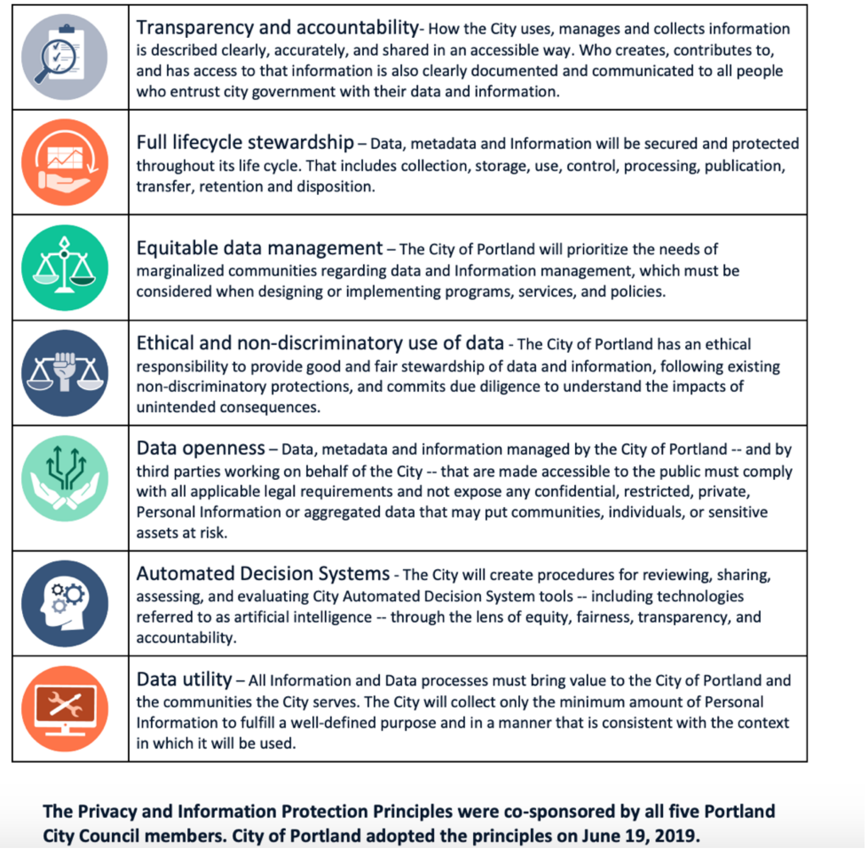
Key Resources

The recommensations in this report were influenced by the city of Portland's Data Privacy and Information Protection Principles and an interview I conducted with Brian Hofer, a civil rights attorney and founder of the Oakland Privacy Advisory Council. Portland was chosen as a key resource because in 2019 the city developed a governing body tasked with adopting and evaluating smart city technologies. Further, the city has placed questions concerning equity and justice as key to their guiding principles. This protocol was spearheaded by the Mayor's Office and the Office of Equity and Human Rights, in conjunction with thirty city agencies and public input provided by community members. According to city officials, these principles are necessary because:

> The City of Portland collects and manages data that may put communities, individuals or sensitive assets at risk. Making the City a more trusted steward of the public's data is a priority of Smart City PDX. Local governments must also plan for emergent information technologies used to better understand and improve government sevices. Providing equitable services related to data collection and

The city developed a comprehensive list of seven principles, which are depicted in the infographic below. While all of these principles are important, I focus on the following for the policy recommendations I put forward:

1. Transparency and accountability
2. Equitable data management
3. Ethical and non-discriminatory uses of data
4. And data utility



	Transparency and accountability- How the City uses, manages and collects information is described clearly, accurately, and shared in an accessible way. Who creates, contributes to, and has access to that information is also clearly documented and communicated to all people who entrust city government with their data and information.
	Full lifecycle stewardship – Data, metadata and Information will be secured and protected throughout its life cycle. That includes collection, storage, use, control, processing, publication, transfer, retention and disposition.
	Equitable data management – The City of Portland will prioritize the needs of marginalized communities regarding data and Information management, which must be considered when designing or implementing programs, services, and policies.
	Ethical and non-discriminatory use of data - The City of Portland has an ethical responsibility to provide good and fair stewardship of data and information, following existing non-discriminatory protections, and commits due diligence to understand the impacts of unintended consequences.
	Data openness – Data, metadata and information managed by the City of Portland -- and by third parties working on behalf of the City -- that are made accessible to the public must comply with all applicable legal requirements and not expose any confidential, restricted, private, Personal Information or aggregated data that may put communities, individuals, or sensitive assets at risk.
	Automated Decision Systems - The City will create procedures for reviewing, sharing, assessing, and evaluating City Automated Decision System tools -- including technologies referred to as artificial intelligence -- through the lens of equity, fairness, transparency, and accountability.
	Data utility – All Information and Data processes must bring value to the City of Portland and the communities the City serves. The City will collect only the minimum amount of Personal Information to fulfill a well-defined purpose and in a manner that is consistent with the context in which it will be used.

The Privacy and Information Protection Principles were co-sponsored by all five Portland City Council members. City of Portland adopted the principles on June 19, 2019.

(Smart City PDX, 2019, p.2)

These principles align most closely with the Feminist Data Manifest-No principles I cite above due to their explicit focus on justice and equity. Portland provides an excellent example of how smart cities can adopt critical interventions that center intersectionality and justice.

Policy recommendations were also inspired by an interview I conducted with Brian Hofer, who is the Chair of the Oakland Privacy Advisory Commission (PAC). In 2016, the City of Oakland created the PAC, which is a citizen-led board that reviews any and all technologies that the city is considering adopting. Oakland was one of the first cities to create a board with such a wide charter and for a few years it was considered the strongest advisory commission in the country. In addition, Oakland's PAC has served as a model for the city of Portland as it has adopted its own principles and the city of San Diego, which adopted a similar civilian-led board following the fallout from the smart streetlight initiative. Due to Oakland's importance within the national technology landscape, my interview with Brian Hofer served as an essential resource for guiding these recommendations.