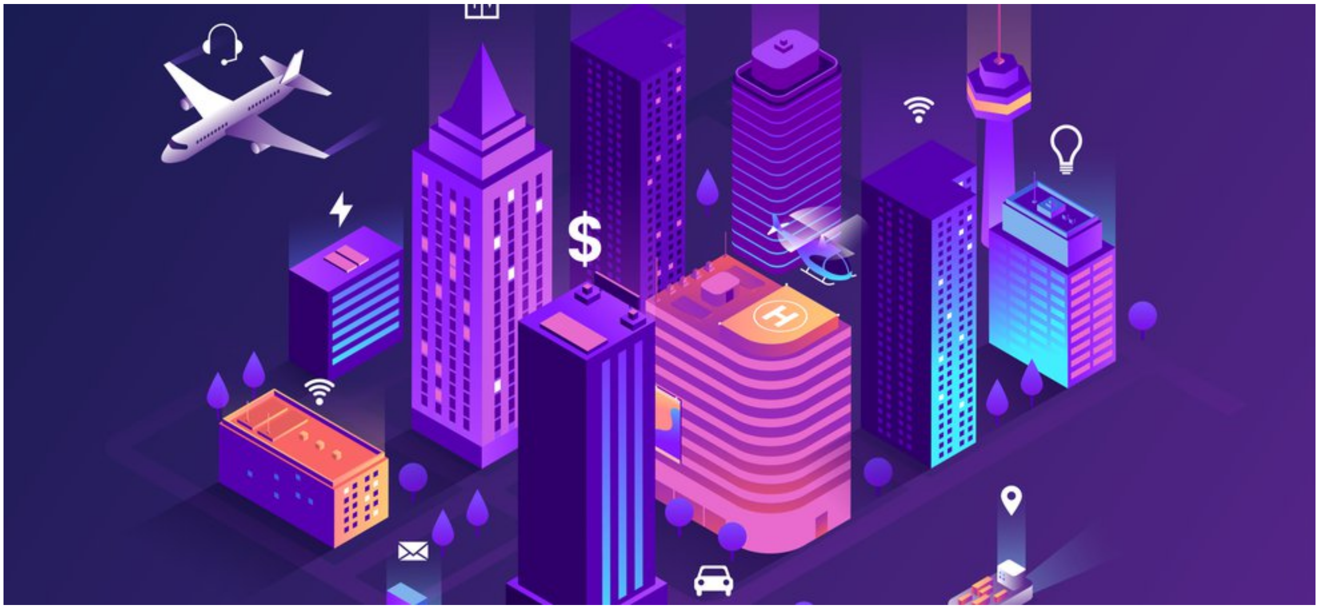
NEW AMERICA



March 2020

A Commons Approach to Smart City Data Governance

How Elinor Ostrom Can Make Cities Smarter

Natalie Chyi & Yuliya Panfil

Last edited on March 05, 2020 at 12:34 p.m. EST

Acknowledgments

We would like to thank Brett Frischmann, Ben Gregori, Elena Souris, David Park, Hollie Russon Gilman, Anne Hobson, Daniel Wu and Tim Robustelli for their assistance with drafting and reviewing this white paper.

We would also like to thank a number of individuals, organizations and workshops that helped conceptualize and develop the ideas in this paper. These include Peter Rabley, Amy Regas, the Ostrom Workshop at Indiana University and its members and affiliates (and in particular Angie Raymond, Scott Shackelford, Michael Mattioli and Greg Bloom), the hosts, attendees and participants of the Human Centered Smart Regions Research Workshop at Virginia Tech University (and in particular Janine Hiller), Sean McDonald, Chris Mellon, Andrew Hagopian, Jessy Kate Schingler and John Wilbanks.

About the Author(s)

Natalie Chyi was an intern with the Future of Property Rights program at New America.

Yuliya Panfil is a senior fellow and director of New America's Future of Property Rights program.

About New America

We are dedicated to renewing America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Future of Property Rights

FPR aims to help solve today's property rights challenges by shrinking the gulf between technologists and policymakers. We also strive to preempt emerging land challenges by thinking critically about the paradigms that govern new spaces.

Contents

Introduction

Smart city projects have made their way onto an increasing number of government agendas globally. These initiatives aim to improve the efficiency of urban spaces, and provide residents with better services in everything from policing to waste management, by enlisting the help of Internet of Things (IoT) sensors and other connected devices. These devices are supposed to make cities "smart" by enabling different state actors to gather and analyze large amounts of citizen data. The data captured may include online activity tracked through Wi-Fi hotspots, location and movement data tracked through a network of sensors, or even biometric information from facial recognition devices.

In a time where concerns about the abuse of personal data and automated decision-making are grabbing headlines, individuals are increasingly uncomfortable with the amount of data gathered about them, and how this data is used and shared. The **Pew Research Center** recently found that over 60 percent of Americans do not think it is possible to go about daily life without private or government entities collecting personal data, and over 80 percent feel little or no control over this data. Most concerning, only 4 percent of Americans **say** they understand what is being done with government-collected data. With private firms such as **Equifax** and **Facebook** suffering major privacy and security breaches, and flawed data use by some **governments**, it is easy to see why the public is worried.

Policymakers are aware of these concerns, but are grasping for solutions. On one end of the spectrum are a set of top-down measures to better protect privacy, whether through data privacy legislation or embedding privacy by design into procurement requirements. On the other are a range of market solutions that call for people to "own" their data as a way of wrestling back control over their information. These ideas are somewhat helpful, but neither is fully satisfying.

Privacy is too narrow a paradigm to fully address the risks that data present, notably biases or inaccuracies during collection and analysis of data.[1] To frame the conversation around privacy is to fence it in, obscuring questions around **broader harms**, and leaving crucial issues unaddressed. Conversely, the suggestion that data should be private property, and that people should own and be able to sell their data, **brings up its own issues**. Commodifying personal information may encourage individuals to license or sell their data for little value, without fully understanding the consequences.

We believe there may be another way, adapted from the work of Elinor Ostrom, to help smart city policymakers fulfil the promise of insightful and efficient smart cities while protecting the rights of city residents.

Applying Ostrom's Approach to Governing Smart City Data

Political economist Elinor Ostrom is remembered for her Nobel Prize-awarded research on the effective governance of commons, which she defined as resources—like water—that are shared and managed by a group. Ostrom's work identifies the conditions that enable groups to cooperate for long-term, successful use of these collective resources through eight design principles situated within an Institutional Analysis and Development (IAD) framework. The application of these principles as an organizational strategy is known as a "commons approach."

Ostrom primarily focused on natural resources, but she extended her theories to digital information at the end of her career, viewing data as a shared resource managed by many. She called this realm the "**knowledge commons**." Over the past decade, Ostrom's work has been taken forward by the **Knowledge Commons Scholars**, who see the emerging digitization of knowledge and information as a way to facilitate a commons approach for its storage, access, and sharing.

We believe Ostrom's approach can be similarly applied to governing data as a resource, and that some of her principles provide insight on how to effectively govern data collected by smart cities.

Ostrom, and the Missing Link of Public Engagement in Smart City Data Governance

Myriad resources provide guidance on data governance, whether for a city's overall data practices (e.g., the What Works Cities certification), for focus on privacy (e.g., GDPR), or for cybersecurity (e.g., the NIST Cybersecurity Framework and Privacy Risk Model). However, none of these resources focus on building or empowering communities to actively participate in governing the data they create, share, and cultivate. In other words, many best practices offer little guidance on the public engagement that Ostrom found key.

Given the criticisms generated by smart city initiatives, including their failure to integrate citizen voices into tech design and implementation, and their failure to obtain consent for mass-scale collection and use of publicly-gathered personal data, Ostrom's work clearly has something to teach cities about transparency and public accountability.

Ostrom developed institutional processes that respond to input from diverse stakeholders who use and steward a resource in different ways. This bottom-up governance approach has several critical benefits: it allows a community to tailor rules to local needs and conditions; it gives community members the autonomy to experiment with diverse rules; and it enables more democratic decision-making, which helps to prevent inequitable outcomes. Ostrom's built-in channels for input allow for better feedback loops, continued evaluation, and a more dynamic system that ensures that rules continue to align and adapt with changing norms.

Our intention is to translate Ostrom's design principles into actions that city managers can take to enable meaningful public engagement around data. Rather than leaving elected representatives or third-party vendors scrambling to impose retroactive guidelines after programs become controversial, we hope our suggestions will help build trust, legitimacy, and accountability from the beginning.

Translating Ostrom's Principles for Smart Cities

From Ostrom's original eight principles, we adapted four that are most clearly applicable to the context of smart city data:

1. Promote responsibility for data governance among multiple layers of nested enterprises.

2. Create processes for the affected community to participate in making and modifying the rules around data.

3. Develop an effective monitoring system to be carried out by the community.

4. Provide accessible means for dispute resolution, use graduated sanctions against rule breakers, and make enforcement measures clear.

Elinor Ostrom's principles for successfully governing a commons	Adapted principles for application to data governance of smart city projects
Ensure that those affected by the rules can participate in modifying the rules.	1. Create processes for the affected community to participate in making and modifying the rules around data.
Develop a system, carried out by community members, for monitoring members' behavior.	2. Develop an effective system for monitoring to be carried out by the community.
Provide accessible, low-cost means for dispute resolution; Use graduated sanctions for rule violators.	3. Provide accessible means for dispute resolution, use graduated sanctions against rule breakers, and make enforcement measures clear.
Build responsibility for governing the common resource in nested tiers from the lowest level up to the entire interconnected system.	4. romote responsibility for data governance among multiple layers of nested enterprises.

Definitions

Before we jump into the principles, let’s lay down a few key definitions.

What Do We Mean by “Smart Cities”?

A **smart city** uses information and communication technologies to increase operational efficiency and effectiveness, share information with the public, and improve the quality of services. To achieve these aims, cities deploy technology across various parts of city infrastructure. These technological systems use distributed sensors to collect data about the environment and city operations; centralized or embedded computing power to process that data; and actuators to manipulate urban infrastructure and adjust city operations. The smart city transforms the city into a large socio-technological system that “senses, thinks, and acts.”

Dubai, London, and New York City are pre-existing cities that have become “smart” over the last decade. Their mayors and/or governments prioritized digital transformation and technological innovation, allowing these cities to become incrementally smarter through different initiatives rolled out by various city departments atop existing infrastructure.

Other smart cities were built from the ground-up,including **Songdo**, South Korea, a joint venture by Cisco and real estate developers, and the **Quayside** neighborhood in Toronto, which is partnered with the Google-owned Sidewalk Labs. What distinguishes these from the examples above is that “the data-gathering infrastructure *[is]* more or less built into the walls,” and done under one cohesive strategy, rather than in piecemeal developments.

What Do We Mean by Smart City Projects?

In this primer, we refer less frequently to smart cities as a whole, than to “smart city projects or initiatives.” This is because we are speaking to any city government or department wanting to implement smart city technology, regardless of whether the city itself is considered a smart city. A city that is just now beginning its journey to becoming smart may actually benefit most from this guide, as it can learn from the experiences of other cities and build correctly from the beginning.

An example of a smart city project is the installation of networks of sensors that measure temperature, humidity, noise pollution, trash levels, energy consumption, traffic flow, and the location of gunshots. These sensors might automatically dim street lights, notify garbage collectors of full trash cans, indicate vacant or occupied spaces on parking meters, or share information on road closures or pollen counts on smartphone apps.

Other examples include deploying a mesh network, rolling out gigabit internet, and providing free Wi-Fi hotspots throughout a city. Some projects involve installing software to perform automated facial recognition or license plate recognition, or include an integrated data center that aggregates existing data from multiple sources into a single facility for monitoring and analysis.

→ EXAMPLES OF SMART CITY PROJECTS:

- **Chicago: Network of sensors**
    - The **Array of Things (AoT)** project comprises a network of sensors installed around Chicago street furniture (i.e., lamp posts, traffic lights) to collect real-time data on factors impacting the city's livability, such as climate, air quality, and noise. This data is published openly for research and public use. The project was funded by a $3.1 million grant from the National Science Foundation, and implemented through collaboration between the city and researchers at the University of Chicago and Argonne National Laboratory. About 130 sensors were deployed in late 2019, with a plan for installation of 150 sensors by mid-2020.
- **New York: Free Wi-Fi hotspots**
    - The **LinkNYC** project replaces phone booths around the city with kiosks that provide free Wi-Fi and phone calls. Announced by the Mayor's Office in 2014, LinkNYC is now built and managed by the private consortium CityBridge (made up of Qualcomm, Intersection, and Comark), which invested an **initial $200 million** needed to build out the infrastructure. It is free and funded by selling ad space on kiosks. However, both the **media** and **nonprofi** have raised privacy concerns.
- **San Diego: Facial recognition technology**
    - San Diego's **TACIDS facial recognition sof** was developed by the San Diego Association of Governments in 2012, receiving $100,000 in funding from the U.S. Department of Justice. TACIDS utilizes a network of 1,300 smartphone and tablet

cameras, as well as a database of 65,500 face scans, for law enforcement use. Described by the California ACLU as "flawed and dangerous," the system was shut down after 2019.

What Do We Mean by "Smart City Data"?

"Smart city data" is data collected by sensors and other technologies deployed in a smart city project, as well as the insights derived from this data.

What Do We Mean by the "Governance" of Smart City Data?

Data governance is not simply data management, or requirements on the collection, use, sharing, retention, and disposal of data, which is codified in data-privacy laws, like the General Data Protection Regulation (GDPR) in Europe and Health Insurance Portability and Accountability Act (HIPAA) in the United States. We view governance more broadly to include questions around who is making these rules and what processes are used in rule making. **Our suggestions do not concern the substance of rules around collection, use, sharing, retention, and disposal of data, but rather focus on how these rules are made, disputed, and changed.**

Our principles are complementary to existing substantive standards around data protection, by providing a procedural component to advance similar goals.

A final note before jumping in: Under each principle below, we describe the range of solutions that may work in any given environment. We encourage you to pick and choose options which would work based on local conditions, as community-unique characteristics will make some more effective or politically feasible than others.

Principle 1. Create Processes for the Affected Community to Participate in Making and Modifying the Rules Around Data.

Ostrom's original principle: Ensure that those affected by the rules can participate in modifying the rules.

This principle speaks to the need for different stakeholders to provide input and collaborate with lawmakers and authorities, so the rules created will best serve local needs and conditions. This is crucial for smart cities, as residents often cannot opt out of smart city initiatives.

For smart city data, "rules" revolve around:

- How data is collected, retained, used, shared, combined, and secured;
- Who profits or benefits from this data, and on what terms;
- Where the technology is located (i.e., sensors); and
- The technology's capabilities.

The goal is to ensure that technology is deployed in ways that reflect and align with a community's self-identified needs. For example, before deployment of surveillance technology by a **police department**, "local input can play a valuable role in ensuring that surveillance policy is consistent with local crime rates, the competence and trustworthiness of the police department, and local political preferences." Failure to account for community input could lead to the adoption of technologies or data policies that are out of step with local preferences, and a subsequent loss of trust.

Community input is also crucial for equity, as the consequences of data misuse will not impact all residents equally: Minorities and low-income neighborhoods are more likely to suffer from poor data governance.

The best methods for engagement, and the expected level of involvement, depend on the characteristics of each community. For example, Oakland, California has a strong tradition of activism, with dedicated citizens spending their evenings and weekends in city meeting rooms, and a high level of concern about police abuse of power. Strategies that work in Oakland may not work in a community that is disengaged politically or maintain a different relationship with the police.

Below are a few questions to guide the creation of more democratic decision-making processes around data.

1. How and where are community engagement processes documented, and how are opportunities to participate communicated to the community?

Both documentation and participation opportunities should follow a "meet-residents-where-they-are" model, and outreach should reflect efforts to include all residents. Ask yourself:

- Is there a documented set of standard procedures for public engagement?
- Where is the public engagement process published?
- Where are opportunities for public participation publicized, and are full details about location and time included?
- How is outreach managed? Are community-based organisations involved?
- Is it clear that all are welcome to participate?

Chicago's Array of Things (AoT) ***Operating Policies****, available on their website, list a public engagement process to be followed before any new AoT nodes are deployed, with a short summary about who must coordinate meetings and what topics must be discuss?*

---

2. How will the city or project engage with the public during the rule creation process? Who is involved, where does it take place, what happens, and when?

There is no single model for engagement, and it is important to match available methods to current needs. Ask yourself:

- **Who is invited?** Is the process open to everyone, or to only a select group, such as an advisory committee of experts or a citizen task force? What is the best way to balance representation with efficiency?
- **Where do engagements take place?** Are physical locations accessible by public transportation? Is an online option available?
- **When are meetings scheduled?** Are meetings during the day or evening? On weekdays or the weekend? Do meetings accommodate a variety of work schedules?

- **What is the meeting structure?** An open house to display technology and answer questions? A series of consultations? Public town hall-style meetings? Or targeted focus groups? What languages are materials provided in? Are interpreters present?

- **What are the expected, or target, outcomes?** To make a decision about whether a technology is deployed? To map and scope potential negative consequences for further contemplation? To determine limits around how technology is deployed? Or to draft some document or policy (i.e., data retention and privacy policy for the project)?

- **Are participants compensated for their time, through stipends for transportation or meals?**

- **How long does the total review period last? How many engagement opportunities occur?**

---

*Seattle's **surveillance technology review process** involves both a public comment period, including release of a new technology's Surveillance Impact Report (SIR) for public feedback, as well as review by the **Surveillance Advisory Working Group**, a standing group of diverse community leaders, that comments on the SIR and conducts a Civil Liberties and Privacy Assessment of the technology.*

---

3. How and where are engagement results documented? How are these results communicated to stakeholders?

Communicating about feed review processes and clearly presenting final recommendations is crucial. Public engagement is most meaningful when organizers are clear regarding how feedback impacts outcomes. Ask yourself:

- How detailed are published results? Are initial comments, incorporated recommendations, and final decisions shared with the public?

- Where are the results published? Only online or physically, as well (i.e., at public libraries)?

- What language(s) are the results published in? Is the writing accessible and easy to understand?

---

*Seattle posts detailed reports from the public comment period for each new technology on their **website**.*

---

4. How are residents involved in changing rules after deployment? Is there any channel for ongoing engagement?

It is crucial to incorporate continued opportunities for engagement following roll out of new technology. New information will come to light during the lifespan of a product or system. There will be unexpected effects. Changes or upgrades will be made to technology or policy. There must be a way for residents to provide input after initial decisions are made. Ask yourself:

- Are there continued opportunities for residents to submit comments or complaints?

- Are there public notifications off future comment periods?

- Are future meetings scheduled to discuss the project? Who is invited?

- Who is consulted on potential changes to the technology or governing policies?

- Is there an effort to build relationships with nonprofits and community leaders?

Principle 2. Develop an Effective System for Monitoring to be Carried Out by the Community.

Ostrom's original principle: Develop a system, carried out by community members, for monitoring members' behavior.

Effective monitoring is crucial to holding decision-makers accountable, and helps to determine when or what intervention might be necessary in the case of a violation.

Monitoring is usually conducted by a mix of NGOs, watchdog groups, media outlets, independent oversight bodies, and industry standard working groups. These actors can track specific projects, actors, types of technologies, or specific civil-liberties issues, conducting investigations and providing reports. Effective monitoring can lead to tangible data governance improvements. For example, Seattle passed its 2017 Surveillance Ordinance in response to strong negative public reaction following the police department's secret acquisition of a surveillance drone and mesh network. The city became aware of this purchase only after NGOs and the media reported on it.

Transparency and reporting are key preconditions for effective monitoring. To that end, smart city projects must be clear about where their technology is deployed and how they aim to use the collected data. Data management policies, privacy policies, and operational protocols must be available to stakeholders, in a language and format they understand. All policies must also be tangible and specific. For instance, privacy policies often use vague language, and might mention sharing data "to improve services," but do not disclose what data is shared, how, and with who.

A written policy that spells out monitoring responsibilities can create more accountability for the project. Chicago's Array of Things website maintains a **map** of sensor deployment, a **list** of sensor types, and an **operating policy**. These resources allow civil society to track sensor locations, potential risks or opportunities, and possible policy violations.

Projects should also publish post-deployment reports summarizing the data collection, use, and sharing. Reporting could take different forms; for example open-data portals, which allow for the bulk download of collected, cleaned, and anonymized data. **New York**, **Louisville**, and **Seattle** maintain city-level data portals, while **Chicago's Array of Things** maintains a project-level portal. However, these efforts only share *what* data is collected, and are silent about how the data is used or shared.

Contracts with third party vendors often impose additional barriers on transparency and reporting requirements. For example, Sidewalk Toronto created a Digital Strategy Advisory Panel, but mandated that they sign aggressive and overreaching **confidentiality agreements**. Non-disclosure agreements are also used by **vendors** to prevent local authorities from sharing basic information about their products. In response, the City of Oakland passed the 2018 **Oakland Surveillance and Community Safety Ordinance**, which expressly prohibits city agencies from entering into confidentiality agreements that conflict with the laws transparency-reporting requirements.

Vigorous and thoughtful oversight depends on a healthy ecosystem of both watchful actors and responsive authorities. Governments can facilitate through financial resources or access to information. Cities can also react more quickly to findings or controversies, such as through creation of positions or offices to draft new protocols. Publicly, cities should build stronger relationships and work more closely with nonprofits and community leaders in order to be aware of emerging issues.

Finally, cities can encourage monitoring by residents through interactive portals. For example, Flint, Michigan's Planning and Development Department created the **Flint Property Portal** in 2017, an online interface where residents can easily collect and report data about blighted properties. Crowd-sourced data allows city officials to better allocate resources for blighted and vacant properties, and also encourages citizens to improve and maintain their properties. Similar initiatives could be applied to the monitoring of smart city technologies, such as the location of sensors or facial recognition software around a city.

Principle 3. Provide Accessible Means for Dispute Resolution, Use Graduated Sanctions Against Rule Breakers, and Make Enforcement Measures Clear.

Ostrom's original principles: Provide accessible, low-cost means for dispute resolution; Use graduated sanctions for rule violators.

1. Provide accessible means for dispute resolution

Dispute resolution and rule enforcement are necessary complements to transparency and reporting requirements. There is no point in publishing an operating or privacy policy if there are no consequences for violating those policies. Written statements are worthless without ways to hold actors accountable.Without ways to hold actors to account, those written statements are worthless.

Create a place, process, and figure responsible for conflict resolution in a manner that stakeholders perceive as fair. Provide mechanisms for rule enforcement and for dealing with bad actors appropriately.

Grievances over smart city projects may come to light after technologies are implemented, or following the release of new information due to monitoring activities. Disputes may arise over data breaches or policy violations (e.g., individuals may complain that their data is used in an unanticipated or impermissible way), or over the location and presence of different technologies (e.g., the existence of an integrated data center, or sensors installed uncomfortably close to a school).

Courts provide one means of dispute resolution. Yet most existing data-protection laws are very limited in scope and accessibility, and therefore are not conducive to court adjudication. For example, many comprehensive data-privacy laws (such as GDPR or CCPA) are directed only at private companies and not government, exempting public bodies from compliance. Other legislation enabling data privacy suits (such as the Federal Trade Commission Act Section 5) does not allow for a private right of action, so individuals are unable to bring claims on their own behalf. Instead, a case would have to be filed by a body like an attorney general or the FTC.

An obvious solution is to amend existing legislation or introduce new legislation that address these challenges. City ordinances have been shown to be effective tools to enforce norms around surveillance technology.[2] Under **Seattle's** surveillance ordinance, for example, the city's Chief Technology Officer can order a stop to the acquisition or use of surveillance technology or its data if any practices violate the ordinances. Under **Oakland's** surveillance ordinance, any individual "subjected to a surveillance technology in violation of this Ordinance" can bring a lawsuit in California courts against the city, and be entitled to recover actual damages.

But not all situations will or should result in litigation, as a matter of practicality and accessibility. Lawsuits take a considerable amount of time and resources which many people cannot afford. If a resident is unhappy about a sensor located right next to their house, for example, this issue may be better resolved through mediation between that individual and those responsible for sensor placement. An impartial third party, mutually agreed upon, can act as judge—perhaps a city-level government official. In a smart city data dispute, the arbitrator may want to take a more hands-on role, such as conducting an impact assessment of the sensor.

The New York Attorney General's Bureau of Internet and Technology (BIT) ***accepts tips and complaints*** *directly from the public, and mediates disputes between consumers and online sellers, service providers, and Internet companies. Could we take inspiration from these procedures, expanding the scope to include government agencies, as well as complaints beyond fraud, deception, or unfair business practices?*

---

2. Use graduated sanctions against rule breakers

Ostrom emphasised the need for proportionate sanctions, or different enforcement actions based on the seriousness and context of an offense.

Sanctions related to smart city data should deter potential wrongdoers and also provide retributive relief to victims. Large fines are effective as a deterrent. On the other hand, ordering a specific action, such as an injunction on the technology, or an order to move its location or alter its data practices, may be more effective at correcting the wrong and providing relief to the victim.

Sanctions should be based on the actual and potential harm suffered, any history of abuse or misuse, whether the violating party was already aware of the problem, and its response, if any.

Finally, transparency and consistency about what types of harm trigger sanctions is key for purposes of fairness and compliance.

Principle 4. Promote Responsibility for Data Governance Among Multiple Layers of Nested Enterprises.

Ostrom's original principle: Build responsibility for governing the common resource in nested tiers from the lowest level up to the entire interconnected system.

In the sections above, we provided recommendations for the improved governance of smart city data. This section seeks to provide guidance on *who* should be implementing the above suggestions.

Cities must create internal capabilities *at multiple levels* in order to understand, support, and delegate responsibility for decisions around smart city data. Designate specific people to make decisions around data, and elevating their roles to positions of power. Educating those already in positions of power about data. Efforts should occur at multiple levels of governance (i.e., city, agency, project, individual), and these multiple parties should be enabled to collaborate or make collective decisions (i.e., through working groups, councils, or committees). This is crucial for shared learning, tracking best practices, and ensuring a coordinated approach between all levels.

Managing data governance in a smart city includes the following responsibilities:

- Evaluating and approving new technologies for the city to develop or adopt;

- Handling public complaints about data and technology projects, and arbitrating data disputes;

- Formulating and monitoring compliance with privacy policies and other relevant legislation;

- Advising and providing internal policy and education within public agencies;

- Increasing public awareness and educating communities on relevant issues; and

- Developing strong relationships with other agencies, NGOs, academia, local communities, the private sector, as well as facilitating communication and convening meetings between these stakeholders.

City-level

Data leadership takes very different forms across different city governments, featuring a range of titles, organizational locations, and responsibilities. At least 16 cities have a **Chief Data Office**r, who sits everywhere from the Mayor's Office in San Francisco to the Department of Innovation and Performance in Pittsburgh. Several cities also have a **Chief Privacy Officer**, **Chief Information Officer** or **Chief Technology Officer**. Most of these titles lack standard definitions. A description of the various roles of city data officers is available **here**, or via an overview of New York City’s ecosystem in **Appendix 1**.

However, evaluating and approving new technologies is not generally a function of these leadership positions, and there is no city-level approval process for technology adoption. As a result, publicly elected city-council members are often in the dark about new technologies their city agencies use, or partnerships that agencies enter into. The results of this awareness gap are painfully apparent in light of recent controversies like the use of the **Clearview AI** facial recognition app by various law enforcement agencies and **Amazon’s Ring’s** secret partnerships with over 500 police departments.

One solution is to delegate the role to an enumerated body. For example, **thirteen cities** have passed surveillance ordinances requiring their city council to approve any city acquisition of technology that meets their definition of “surveillance.” It is important that this oversight covers not just formal acquisitions of technology, but also free software (i.e., Clearview AI) or informal partnerships (i.e., Amazon Ring).

While a city council may make the final decision, cities could also create or use expert groups to advise the council’s decision making. For example, Oakland’s standing **Privacy Advisory Commission (OPAC)** is made up of community experts who provide advice and technical assistance on best practices to protect citizen rights in connection with the City’s purchase and use of technology that collects or stores citizen data. A city may also tap a party with some pre-existing expertise, notably a Chief Privacy Officer, to play a greater role in the technology adoption process. A city may also want to invest in programs like **civic fellowships**, or lean more heavily on NGOs and foundations already working on these issues.

Agency-level

City agencies and departments that routinely roll out smart city technology, or even those that do not, may wish to create their own officer position, informal working group, or advisory committee to evaluate new technologies and data policies prior to adoption.

The U.S. **Department of Justice** urges all law enforcement agencies collecting personally identifiable information (PII) to have a Privacy Officer, and New York City's **Identifying Information Law** requires each agency head to designate an individual to act as its privacy officer that will compile and report information about their agency's collection and disclosure of identifying information, as well as their privacy practices. However, these officers' roles largely relate to reporting. While transparency is important, in the case of technology adoption it is also crucial for these individuals or committees to have decision making power —perhaps working—closely with or inside procurement departments.

Project-level

Each smart city project must also take responsibility for key data governance issues. Each project should have a designated leader responsible for developing project-wide data governance practices and policies, and dealing with any conflicts that arise. The city government could facilitate the creation of this role by making this designation a prerequisite of project approval, providing advisory support to project teams, or connecting the team to NGOs that could help in an advisory capacity.

Individual-Level

At the lowest level, individuals should have input into the activity through public comment periods, town halls, proceedings open to the public or as part of a multistakeholder proceeding like a working group open to the public. (As elaborated upon in Principle 1.)

Appendix 1

Below, we take a look at the main players in NYC's ecosystem of data leadership as an example of how a city has currently put together an ecosystem of tech-focused public servants.

Office	Lead	Responsibilities
Mayor's Office of Information Privacy	Chief Privacy Officer	Creating new privacy policies and protocols for the City / within a comprehensive citywide information privacy protection framework
Mayor's Office of Technology and Innovation	Chief Technology Officer	Development and implementation of a coordinated citywide strategy on technology and innovation, and encouraging collaboration across agencies and with the wider New York City technology ecosystem.
Mayor's Office of Data Analytics (MODA)	Chief Analytics Officer	Collaborating with City agencies to implement data-driven solutions to City service delivery issues, building a Citywide data platform to facilitate data sharing, overseeing Citywide Data Projects, and implementing the City's Open Data Law.
New York City Department of Information Technology and Telecommunications (DoITT)	Commissioner of the DoITT	Establishing the City's IT strategic direction and security standards, modernizing the City's IT infrastructure and procuring citywide IT services, evaluating emerging technology, and using innovative solutions to improve the delivery of City services.
Bureau of Internet and Technology (BIT) of the New York Attorney General's Office	Attorney General	Bringing cases to protect consumers from developing online and technology threats, drafting legislation on emerging technology issues, and educating the public on Internet matters.

Notes

[1] Collecting data that are non-representative of reality,due to being limited in size or diversity, or reflecting historical human bias, has led to discriminatory results suffered by the most disadvantaged groups. For example, various studies have shown that facial recognition software is often inaccurate, which could have unjust consequences when used in law enforcement systems.

[2] The ACLU Community Control Over Police Surveillance (CCOPS) campaign provides a set of guiding principles and template model bill language for surveillance ordinances.

This report carries a Creative Commons Attribution 4.0 International license, which permits re-use of New America content when proper attribution is provided. This means you are free to share and adapt New America's work, or include our content in derivative works, under the following conditions:

• **Attribution.** You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

For the full legal code of this Creative Commons license, please visit **creativecommons.org**.

If you have any questions about citing or reusing New America content, please visit **www.newamerica.org**.

All photos in this report are supplied by, and licensed to, **shutterstock.com** unless otherwise stated. Photos from federal government sources are used under section 105 of the Copyright Act.