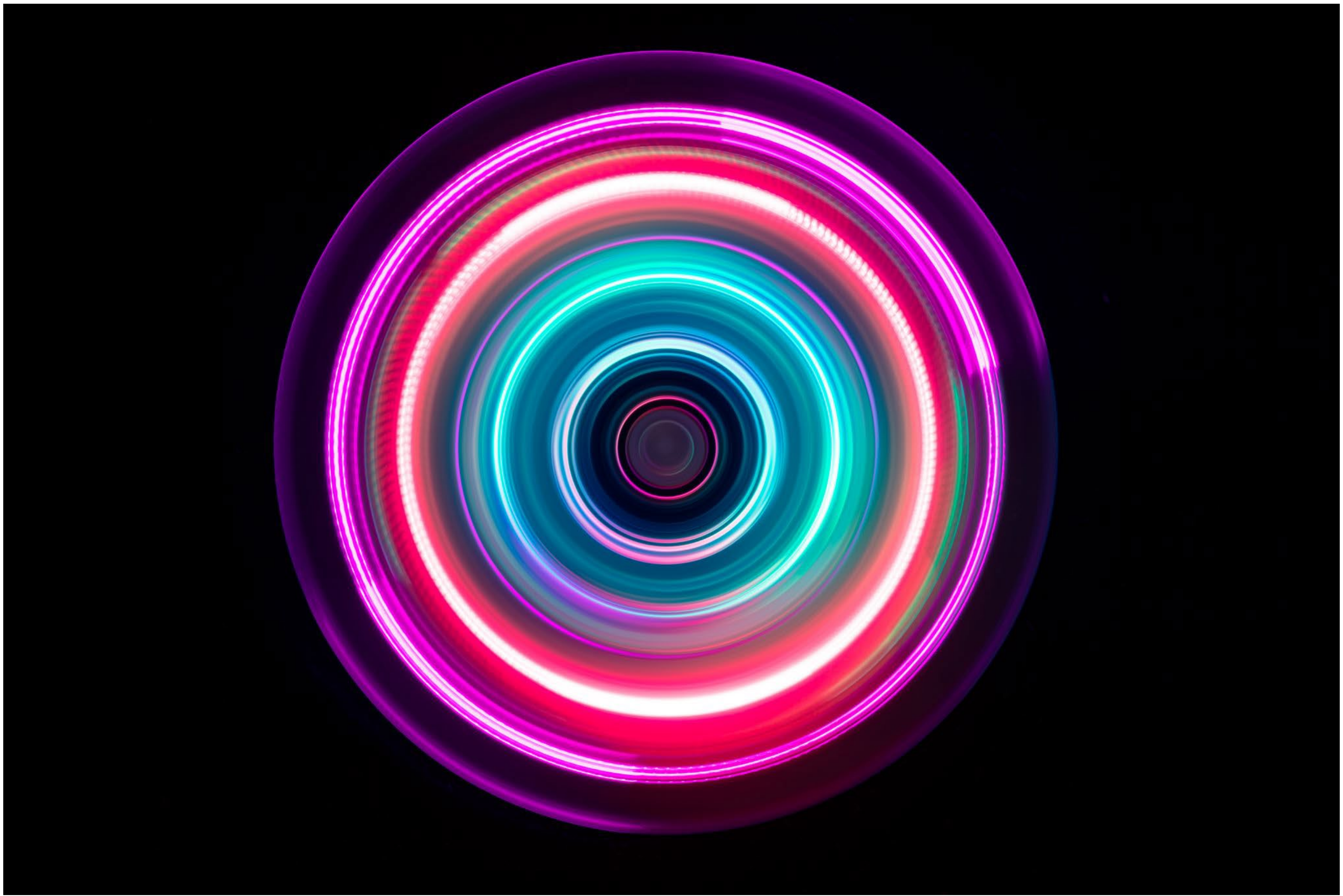
BEING WATCHED

BEST PRACTICES FOR EMBEDDING ETHICS, TRANSPARENCY AND ACCOUNTABILITY IN SMART CITY SURVEILLANCE TECHNOLOGIES

GOOD SYSTEMS, UT AUSTIN

Date Released: Draft from August 2024

Table of Contents



OVERVIEW

Camera-based surveillance technologies that are deployed by cities or that cities have access to through public-private partnerships include traffic cameras, High Activity Location Observation (H.A.L.O) cameras, red light cameras, CCTV cameras, automated license plate readers, dash cameras, body-worn cameras, drone cameras, and ring cameras. The use of these systems is increasing around the world. Enabled by network communication systems and existing within an infrastructure that includes control rooms or monitoring centers, these technologies generate public and private video feeds accessed by municipal services in the conduct of business and frequently the subject of artificial intelligence-driven analytics. Drawing from existing public data principles and data governance instruments alongside the knowledge base of the records and information management profession, this White Paper sets out ethical, transparent, and accountable guidelines for surveillance technologies and resulting data that acknowledge and take into consideration the needs of varied smart city stakeholders.

Executive Summary

Acoustic detection systems, street-light cameras, automated license plate readers (ALPRs), body-worn and dash cameras, and unmanned aerial vehicles (drones) are camera-enabled 'Smart City' technologies deployed to improve outcomes in urban planning, environmental monitoring, and public safety.[i] Examples of the deployment of cameras in public settings include local housing agencies' use of camera systems to watch over public housing facilities, local police departments' use of license plate scanners at city intersections to locate vehicles of interest, and municipal governments' use of cameras to monitor pollution from construction sites.[ii] In the US, support and funding for such systems are facilitated by federal monies, including from the U.S. Department of Justice, the Department of Homeland Security, and the Department of Housing and Urban Development's crime-fighting grants.[iii]

As data capture, collection, and transmission devices deployed in urban spaces, cameras can record and store real-time video, audio, and still images. As visual sensors, cameras deliver actionable data about human behavior to optimize infrastructure, resources, and spaces with the potential to archive, and make information public through open data portals. Alongside sensors, microphones, meters, and beacons, cameras are embedded in networked systems and linked to smart applications with data analysis capabilities.[iv] With the help of built-in and associated analytics, data related to objects, events, and changes can be extracted, transformed, and processed. Markers or identifiers can be used to flag features like location, time, movement, and size within video streams. Add-on capabilities or services, often utilizing machine learning algorithms and computer vision, allow for "object detection and tracking, object classification and recognition, event detection and prediction, behavior recognition, video summarization," and the like.[v]

The presence of cameras in our society and what to do with the data captured as a result is a complex issue involving conflicting rights and interests. While smart city camera systems are tools to promote public safety and protect resources, they also can have a negative and disparate impact on civil rights and civil liberties. Concern for how personally identifying data is being collected and used has led to checks on the use of cameras and associated technologies, including actions in Alabama (AL SB56 2022) and California and Washington to limit the use of AI and facial recognition by state and local entities, along with a raft of city "surveillance ordinances" designed to guide decisions about using such technologies and the data they produce toward public oversight. There is a growing demand for transparency and accountability (including oversight measures) around data collected by smart city technologies, which is complicated by competing public and private stakeholder interests.[vi]

As the use of public cameras increases, the need to develop and promulgate robust policies regarding their use takes on new urgency. This White Paper offers an advisory framework to help municipal entities create a balanced approach to the deployment of smart city cameras and the retention and disposition of resulting data that acknowledges the needs of smart city stakeholders. In particular, the White Paper presents emerging best practices that foreground issues and principles of transparency, accountability, and ethics. In government settings, data retention policies are operationalized through records retention schedules, emphasizing the administrative, legal, and compliance drivers for what must be retained and destroyed.

The need to broaden perspectives on surveillance technologies and the data they produce to include a specific ethical lens is borne out by examples of scattershot camera policy updates that look to prevent situations and conditions where the experiences and outcomes of surveillance technologies could or do result in harm to the public and instead find solutions where transparency and suitability of purpose come to the fore.[vii] Events in Detroit, where community opposition to the use of facial recognition systems in Detroit catalyzed a formal governing ordinance, and residents' objections in San Diego to the use of camera-equipped streetlights – which also led to a surveillance technology ordinance – are prominent examples of why cities should be proactive about involving communities before acquiring and using these systems.[viii]

Responsible oversight and control over the systems that put smart city technologies in place and circulate and use the resultant data are needed. This White Paper posits that systems oversight and control are based on having foundational knowledge of five overarching substantive issues to feed into smart city policies:

(1) the goals of city government in deploying smart city cameras in public spaces,
(2) the stakeholders, including residents, who are impacted or can have an impact on the deployment and use of cameras and associated data,
(3) the lineage and
(4) risks associated with camera data across its lifecycle, and
(5) an overarching ethical lens to clarify how municipal governments ought to act when making assessments through these four analytical approaches.

The following four analytical frameworks can address these issues (see Table 1).

Functional Analysis	***Stakeholder Analysis***	***Risk Mitigation Analysis***	***Data Lifecycle Analysis***
Articulating the functions and activities in public spaces that result in smart cities' camera data generation and management. ***A functional analysis should include a detailed, documented, and agreed-upon list of the functions, activities, and processes in which smart city cameras are typically employed, which can later be augmented with a listing of the accompanying structured and unstructured data that emerge from these processes.***	Considering stakeholder-defined data control models and opinions regarding the business, administration, economics, and social values of camera-based surveillance technologies and resulting data. ***A multi-faceted stakeholder analysis should identify the interests, power, and differences among the various stakeholders, and how their needs align with the mission and vision of municipal entities as they operate within a smart city environment***	Working in concert with legal and regulatory requirements, industry standards, and local policies and processes impacting technology adoption, business functions, and data and data governance issues. ***Risk mitigation analysis addresses two main concerns. The first concern is the potential impact of monitoring and surveillance technologies on civil rights and civil liberties, which poses potential harm to specific groups of people. The second concern is the need for public access to records generated by smart cameras, which is essential for transparency in governmental functions and activities.***	Mapping of public data as it moves through the stages of creation, streaming, use, reuse (including instances of proactive or reactive disclosure), sharing, long-term retention, and deletion. ***At its most basic, understanding the lifecycle of data involves delineating data types and what happens to that data from creation/ generation, to collection, preparation/ processing (categorization, organization, transformation, analysis, and visualization), deployment/use, sharing, storage, and disposition.***

Table 1. Four Analytical Frameworks for Developing Ethical Smart City Policies.

Our goal here is to explore aspects of each framework in order to share what each one emphasizes. No single framework can satisfy all the questions and issues that may arise, but this discussion can foreground the range of possibilities and suggest some paths forward. Using the frameworks should foreground the ethical decisions and presumed outcomes that can be obtained by conscious and deliberate assessments of AI-enhanced technologies.

Background

City spaces comprise localized community neighborhoods and electoral divisions (wards, boroughs, precincts, districts, and quadrants) that come together to form the urban landscape. The landscape of cities generally radiates out from downtowns and business districts, with larger metropolitan areas characterized by distinctive inner-city neighborhoods, sprawling industrial estates, specialized economic zones, and lower density suburban communities. According to the United Nations, nearly seventy percent of the world's population will live in urban areas by 2050.[ix] In the United States, since 2000, ninety-eight percent of the growth in population in the one hundred largest cities was from minority populations.[x]

The quest to transform cities into smart cities taps into solution-oriented imaginings of the city. In this conception, growth can be accommodated alongside improvements in the quality and safety of urban life and in the infrastructure vital for economic development. In the United States, real estate technology company ProptechOS lists Austin, Los Angeles, Seattle, San Francisco, Atlanta, Oakland, Boston, New York, San Jose, and Miami as the cities best prepared for such a ‘smart city future.’[xi] At the core of the smart city vision is widespread technology deployment, allowing actionable urban data to be collected and extracted from the city’s residents and environs. Smart city technologies exist in what Rob Kitchins describes as the domain of governance and governmentality, and the associated temporalities of “real-time, optimization, efficiency, longitudinal analysis, pre-emption, anticipation, predication, [and] forecasting."[xii] As researchers Bibri and Krogstie note, smart cities rely on "constellations of instruments across many scales that are connected through multiple networks augmented with intelligence, which provide and coordinate continuous data regarding the different aspects of urbanity in terms of the flow of decisions about the environmental, economic, social, and physical forms of the city."[xiii]

Smart city technologies rely on a base of detection devices, often called an Internet of Things array, that empower the sometimesreal-time, sometimes recorded awareness and data aggregation necessary to drive insight and innovation. Cameras and other sensors (some that can detect the movement of objects and others that measure noise, pressure, temperature, humidity, airborne particulates and gases, and chemicals in water and the air) are a key part of this municipal Internet of things. These sensors are put to work to sustain city functions, including public safety, environmental monitoring, urban mobility, and emergency response.

In the case of cameras, geographic placement locations are tailored to provide visual data on roads and other physical features of the urban landscape alongside the human and non-human objects (e.g., vehicles) that move within their sphere. Overall, cameras serve as devices to enhance security (monitoring to prevent acts of human malice towards goods, people, and places), safety (monitoring to protect people and property from accidents and disasters), and surveillance (watching over behavior and activity to detect, control, and/or gather evidence of activity). By the same token, some cameras, such as body-worn cameras on police, facilitate a reciprocal or accountability check on public safety-related behaviors.

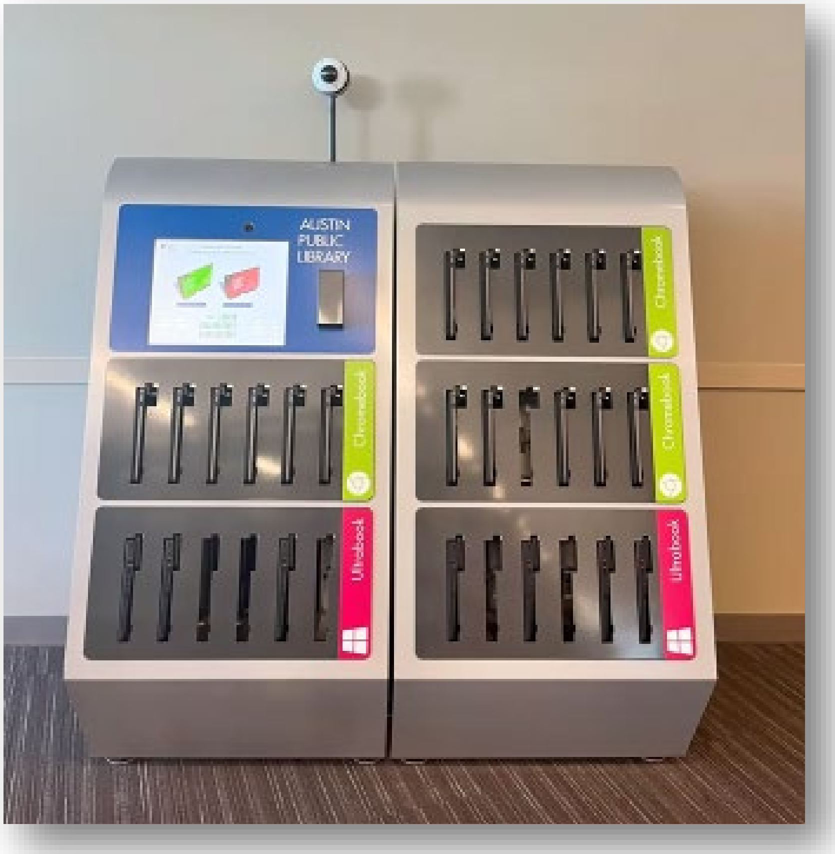


Figure 1. Laptop Checkout Kiosk with Camera, Austin City Library

Cameras deployed in smart city contexts are both fixed and mobile. Fixed bullet, dome, turret, fisheye, thermal, high activity location observation cameras (HALOs), and pan-tilt-zoom cameras are deployed on-premises and in the built environment (e.g., on power poles, streetlights, traffic signals, parking lot entrances, and exits). Mobile cameras are deployed as part of unmanned aerial vehicles (drones) and with robot, vehicular, hand-held (e.g., situational awareness cameras), and body-worn configurations. Deployed devices include internet protocol (IP) cameras with no local recording hardware or with some local storage, generally communicating images through a network to either a control center or into a file for software analysis.

With the mantra of 'what can be monitored can be managed,' these devices collect and compress video footage transmitted over an IP network to monitoring stations. IP cameras generally allow live viewing, continuous recording and recording on a schedule, or recording triggered by an event. AI-enhanced IP cameras integrate software programs with facial recognition, database matching, and vehicle and crowd-counting services. Alternatively, deployment of edge computing - computing at or near the data source through stand-alone devices connected to cameras - allows the data (including captured video and metadata) to be preprocessed locally in real time for volume reduction, analytics, and other workloads (see the Intel® Video AI Box platform as an example).[xiv] From there, data can be transmitted to a centralized system. AI services make it possible to index and search large amounts of video data by summarizing information and detecting and finding patterns in human features (age, gender, faces), objects, emotions, events, and behaviors. With the latter, this involves examining trajectories, motion patterns, and pathways to identify anomalous or unwanted actions such as fighting and loitering.

Video data, however, is not without its problems. Issues with camera data coalesce around concerns with data quality, alongside the risks associated with amassing, aggregating, analyzing, sharing, and retaining information about people and their environments. Some of the potential hazards are related to safeguarding privacy, avoiding data surveillance, insuring appropriate accuracy and reliability of these systems, preventing data discrimination, and mitigating the risk of data breaches. Tools to mitigate some of these risks include vendor management programs, local data storage infrastructures, data privacy regulations, data minimization policies, transparency and consent processes around data collection and use, and data de-identification practices.[xv]

***In light of the widespread deployment of camera-based surveillance technologies in smart cities, this White Paper focuses on key decision points in systems oversight and control where notions of government transparency, accountability, and ethics come into play*.**

While roughly 23 U.S. cities have formal ordinances regarding surveillance technologies and many more municipal entities have internalgoverning policies regarding the retention of the analog and digital records that emanate from functions and activities of city government, the same cannot be said for the data that emerges as part of the smart city vision.

Historically, there have always been many records generated by city units, but what is new now is the large volume of data the city produces through these new technologies.

At issue is that retention decisions have traditionally been aligned with the voluminous information outputs of city government (records) rather than the equally or greater volume of data that begins as raw information input from proliferating surveillance technologies.

The four analytic frameworks we discuss can guide how one should think about handling the data produced by smart city-style technologies. Each prioritizes certain kinds of outcomes and ethical considerations.

Functional Analysis

In the United States the city operates as a system of systems, providing increasingly smarter services to a growing number of city units and citizens. By engaging in core functions and activities, smart cities try to align their mission and vision with the challenges of urban living. Overall, the functional responsibilities or scope of city government involves the management of the physical, civic, economic, and social infrastructure that holds communities together in the form of economic development, urban planning, transportation and utilities, environmental monitoring, waste management, public safety, health and human services, public housing, parks and recreation, and cultural and arts programming. Using an ethical lens in this context requires mindfulness and observance of the overarching goals and values of cities as specific forms of governmental arrangements. The overarching goal of cities, in this instance, is to perform services that advance "the interest, welfare, health, morals, comfort, safety, and convenience of the city and its inhabitants."[xvi]

What is the purpose of city government?

How does it perform its business?

How does legislation, regulations, and other mandates govern the way that smart cities function and operate?

How and why do smart city technologies play into strategic objectives?

To understand the goals of city government in deploying smart city cameras in public spaces the functional analysis method can be used as a baseline tool to distinguish and document the core functions and activities in which smart city cameras are deployed. As part of an information governance team, records management personnel typically can make such determinations in conjunction with program or policy analysts. As a form of assessment, functional analysis draws out what an institution (in this case a city) does and how it carries out its work, linking functions and activities to broad governing mandates and to the data that emerges from the process.

For the purposes of this White Paper, functions are the largest business activity units designated to city governments and directed to specific ongoing strategic goals and objectives. Activities are the recurring tasks the city performs to accomplish its functions. Processes are activities or clusters of activities carried out by people and systems to produce a defined outcome, often involving the creation and circulation of records in the form of unstructured (e.g., video) and structured data.

Evidence of a city government's purpose, functions, and activities can be found within the municipal information environment. In cities with a home-rule form of government, charters act as constitutions, laying out their organization, powers, functions, and essential procedures.[xvii] The preamble to the City of Austin's charter ("*We the citizens of Austin, in reverence to the dignity and the enrichment of all people, do ordain and establish this Charter to assure economic, environmental, and cultural prosperity throughout our community")* captures how community proprieties, norms, and values are inscribed within these texts. City ordinances are a type of authoritative action, rule, or regulation not already covered by state or federal laws that provide granular details of public policy and, more specifically, how cities should operate. City ordinances are created through deliberative processes that include public comment and feedback before being enacted in municipal codes.[xviii] When it comes to data, contemporary interests in transparency in gathering and using data are prominent.

As a functional analysis will discern, the adoption and use of cameras and camera data in public spaces likely occurs in the context of fulfilling the approved local government purposes of public safety, emergency response, and transportation operations. These functions are often spread across various city departments. In the case of the City of Austin, for example, the security of property and people falls wholly or partly within the purview of Police, Fire, Transportation, Parks and Recreation, Building Services, Public Health, Public Libraries, Austin Bergstrom International Airport, and the Austin Convention Center.

Transportation Operations	***Public Safety***	***Emergency Management***
• Traffic management and monitoring (traffic flow - car count/frequency/direction, journey time analysis, optimal bus routes) • Traffic rule violation detection and enforcement (monitoring of reserved lanes, bus lane enforcement) • Parking management (parking lot occupancy detection) • City planning (city modeling, urban-rural classification and planning, corridor mapping)	• Law enforcement - preventing, detecting, and investigating criminal activities (deterring crime, detection of stolen and wanted vehicles, perimeter monitoring, intrusion and threat detection, weapon detection and reporting, hostage/crisis negotiation, loitering detection, securitization of tunnels and bridges) • Maintaining public order and safety (event and crowd management) • Officer oversight (officer transparency and accountability, including supervisory and performance reviews)	• Monitoring of critical infrastructure and key resources (CIKR) (roads, communications, water, energy) • Natural disaster (wildfire) monitoring • Detection of the impact of critical weather events on humans, air quality, etc.

Table 2. Functions and Activities of City Government in Which Smart Cameras are Typically Deployed.

Adding smart city technologies aims to augment these existing practices, moving people and goods through the city in faster, safer, sustainable, and more equitable ways. As highlighted in Table 2, cameras are generally deployed in activities involving monitoring, identifying, enforcing, protecting, and preventing. The emphasis here is on gathering tactical intelligence on people, vehicles, and the built environment to help create secure, connected, and resilient communities. In particular, camera usage has gained traction where real-time situational awareness of monitored activities is a demonstrated asset.[xix] Visual imagery, for instance, “can provide first responders, dispatchers and supervisory personnel with important information on the nature of any incident, whether an emergency or a routine public safety response,” with this data often centralized to handle the volumes of data from an ever-changing target environment.[xx]

A functional analysis should include a detailed, documented, and agreed-upon list of the functions, activities, and processes in which smart city cameras are typically employed, which can later be augmented with a listing of the accompanying structured and unstructured data that emerge from these processes. In doing so, insight can be gained into how city government supports the adoption of smart city technologies and how that adoption plays out as part of their stated purposes and values. In sum, the core functions and activities of a city provide the rationale for the generation of smart city camera data. A clear alignment between city functions and civic goals, and how smart city projects fit within these frameworks, should serve as the foundation for any discussion of how smart city data should be managed across its lifecycle.

Stakeholder Analysis

Identifying those invested in camera-enabled 'Smart City' technologies and their attendant data is the next prerequisite for envisioning data control models in which data disposition is linked to appropriate business, administrative, economic, and social requirements. From an ethical perspective, it is also a prerequisite for transparent and accountable city governance. Undertaking a stakeholder analysis should be done with the understanding that smart city audiences and their interests may vary across the technology and data lifecycle.

Who are the key audiences and stakeholders across the lifecycle of smart city cameras and their associated data?

What are the interests of these stakeholders? What are their concerns and interests in smart city issues?

Where do stakeholders fall in the matrix of roles of those who are responsible, accountable, consulted, informed (the RACI matrix)?

What are their values, commonly held principles or valued qualities (business efficiency, economic development, personal safety, freedom, fairness)?

In the case of smart camera technologies and data, broad stakeholders include city government representatives (depending on the form of local government this may include city mayors, councils, commissioners, managers, boards and commissions); city administrative departments and offices (including police, planning and development, housing and community development); city technical implementers (e.g. procurement, IT), labor unions that represent city workers; policymakers and supervisory agencies (e.g. state legislators, state and local data liaisons, records managers and archivists); policy services and policy management software companies (e.g. Lexipol); corporate entities that enter into public-private partnerships for smart city purposes (including technology vendors, commercial builders, and developers); lawyers, journalists and the media, civil society activists (including special interests groups and public interest research groups in the areas of privacy and civil liberties - e.g., American Civil Liberties Union, Electronic Frontier Foundation, Electronic Privacy Information Center, Privacy International, and the Sunlight Foundation), and the individuals and community partners (neighborhood associations, etc.) that live and interact within Smart City environs (see Table 3).[xxi]

The interests of the various stakeholders can be further determined by articulating how people connect to smart city camera issues. Stakeholders can be sorted into passive and active categories. From a community standpoint, engagement in civic life is facilitated by government communication that keeps residents informed; through community conversation that brings the public into the deliberative process; through public consultation and input via public comment periods, public hearings, and community surveys and polls; and through collaborative and sustained public problem solving where the public is a part of community advisory committees and task forces.[xxii]

So-called passive stakeholders are those that are affected by but do not traditionally have power over or contribute to deploying smart city camera technologies. Their role is often discretionary. However, engagement can occur through official or designated representatives, including third-party advocacy groups, that have a greater ability to support or recommend a particular cause or policy. Active stakeholders are those that directly contribute to or influence the deployment of smart city camera technologies. Some cities have actively cultivated community engagement to solicit input on data policies.[xxiii]

Functions and Activities	Stakeholders
Transportation Operations traffic management and monitoring, traffic rule violation detection and enforcement, parking management, city planning	• Policymakers and records/data supervising agencies • Management, operational users (real-time and/or forensic access), and technical implementors in city agencies • External data recipients (e.g., regional public safety agencies) • Private sector partners • Lawyers, civil society activists • Media • Community partners • The public
Public Safety law enforcement, maintaining public order and safety, officer oversight	• Policymakers and records/data supervising agencies • Management, operational users (real-time and/or forensic access), and technical implementors in city agencies • Regulators and civilian boards • Courts and lawyers • External data recipients • Police unions • Commercial entities with public safety concerns • Lawyers • Civil society activists • Media • Property owners • The public
Emergency Management monitoring of critical infrastructure, natural disaster monitoring, detection of the impact of critical weather events on humans, air quality, etc.	• Policymakers and records/data supervising agencies • Management, operational users (real-time and/or forensic access), continuation of operation personnel, and technical implementors in city agencies • External data recipients (e.g., regional public safety agencies) • Private sector partners • Media • The public

Table 3. Functions and Activities of City Government and Associated Stakeholders.

Using the RACI or responsibility assignment matrix concept from project management provides clarity on where responsibility and accountability are vested (including the idea that city governments are moral agents responsible for the impact of smart city technology on individuals and the community) versus who needs to be consulted (representative stakeholders) and/or kept informed.

From a technological perspective, stakeholders can be demarcated in terms of who implements, who uses, who is affected (harmed or benefited) by, and who is interested in camera-enabled technology and its resultant data. From a data perspective, stakeholders can be demarcated in terms of who is affected (harmed or benefited) by the data, who uses and reuses the data, who manages the data, who owns the data, and who stores the data. Guiding questions regarding the effect of smart city camera technologies include:

Which individuals or groups may encounter harm, suffer losses, or face damages because of the implementation of smart city cameras and the dependence on the data produced by these systems? Which individuals or groups could benefit, acquire gains, or turn a profit due to deploying smart city cameras and relying on the data generated by these systems?

Losses at the individual level could refer to infringements on privacy rights and those of free association, while losses at the organizational level speak to operational, financial, and reputational risks including trust in the city by the public.

Another important issue in stakeholder analysis is looking to the municipal information environment to clarify competing stakeholders' wants and needs. Potential conflicts can be seen, for instance, between the need for data to be captured and processed as part of the core functions and activities of government agencies (e.g., gathering evidence for law enforcement purposes) versus the need for data to be captured and processed according to external needs and demands, including for privacy purposes, research purposes and purposes of government oversight and accountability.

For example, city government officials and administrators seek real-time information for current and future decision-making and efficiency, effectiveness, and innovation in delivering goods and services. While the business framework for smart city technologies speaks to enhancing and augmenting existing practices, some external stakeholders argue that the effect of widescale camera deployment as a surveillance mechanism is so substantive that additional transparency, community engagement, formal oversight, and/or local regulation is required. The claim is that some smart city technologies undermine faith in how cities carry out their core functions and activities and what is achieved in the process.

There is also a concern that, once deployed, smart city technologies can be used beyond their original remit. An example is video-equipped smart streetlights in San Diego being deployed as a transportation aid while the raw camera footage is made accessible as part of police investigations.[xxiv] With the input of non-governmental organizations and stakeholders, municipalities have enacted governance structures with a range of policies (the 'what'), principles (the 'why'), and procedures (the 'how') that prioritize creating functional and equitable cities for all residents, including in the realms of data privacy, civil liberties, adopting and using surveillance technologies, and reimagining public safety.[xxv] ***In this context, transparency refers to the idea that citizens have the right to be informed while accountability signals a desire for oversight over what is happening in government, from federal to local levels.***

Consideration must also be given to conflicts that can occur within a stakeholder community. For example, some city residents see smart-camera technologies and their associated data streams as important tools to enhance security and safety. Indeed, as part of the constellation of smart city technologies, city governments can implement what Michael Kwet calls "plug-in surveillance networks," in which residents place privately owned cameras on city networks. The Project Green Light in Detroit is an example of a police-business program in which businesses install camera systems to police specifications and in return receive privileged policing services. Other private-sector camera initiatives have occurred in Atlanta, Chicago, San Francisco, New Orleans, and New York.[xxvi] However, residents have also expressed concern about the surveillance capabilities of smart-camera technologies and questions of who within the community can access the data subsequently.

Indeed, it must be noted that requests for data may be made for various purposes, including criminal investigations, legal proceedings, media inquiries, and private interests, including individuals and entities whose activities or property may or may not be represented. As the ACLU notes, “the public should have access to the same information as the government; however, such access also means that widespread video surveillance systems can quickly prevent people from keeping their activities private, not just from the government, but also from other private parties.”[xxvii] In disseminating video data, concerns are paid not only to access for the purposes of transparency and open government but also to the need for redaction to protect privacy and facilitate the criminal justice process. As the U.S. Department of Homeland Security Science and Technology Directorate notes regarding video, “While redaction issues can arise in any dissemination context, it is most likely to occur in response to FOIA or open records requests. Responding to these requests will require not only personnel, but also additional software and perhaps hardware to redact responsive data. The question of redaction may involve not only imagery, but also audio data and associated metadata.”[xxviii]

Overall, in conducting a multi-faceted stakeholder analysis, the goal is to identify the interests, power, and differences among the various stakeholders, and how their needs align with the mission and vision of municipal entities as they operate within a smart city environment. With this information in hand, cities can better plan for how stakeholder concerns can and should be incorporated into the process of managing smart city cameras and resulting data across its lifecycle.

Risk Mitigation Analysis

In carrying out their functions, cities are also bound by external requirements, including federal and state law alongside the standards and best practices the community expects municipal governments to meet.

The first concern is the potential impact of monitoring and surveillance technologies on civil rights and civil liberties, particularly with respect to the First, Fourth, and Fourteenth Amendments to the Constitution. This is due to the potential harm caused by data collection and retention on specific groups of people. The second concern concerns the need for public access to records generated by smart cameras, which is essential for transparency in governmental functions and activities. In the context of smart cities, this means that, alongside paper records, local governments should provide access to digital audio and video files in compliance with public records laws. However, the current landscape of state public records laws is such that there is no guarantee that localities will provide the public with access to records about and produced by Smart City technologies. [xxix]

Instances where cities and communities have discerned that the risks of deploying smart camera technologies and associated applications outweigh the benefits (including in cases of city liability and diminished trust in city government) have led to regulatory ordinances that scale back their scope of use and limit the acquisition and use of information derived from the technology. Local bans on the use of face recognition technology due to privacy, racial bias, and civil liberty concerns are a prime example, with seventeen cities in the United States having enacted such ordinances as of 2022.[xxx]

Driven in part by smart city and open data initiatives, local privacy laws, ordinances, resolutions, regulations, and policies (with the cities of Seattle and New York notable examples in this regard) focus on regulating the procurement and use of surveillance technology and equipment alongside the regulation of city agency's collection, use, disclosure, sharing, and retention of the personal data of city residents. For example, the City of Seattle's collection, sharing, and use of data is guided by a set of privacy principles and adheres to the State of Washington's Public Records Act, Washington State Record Retention Law, and the City of Seattle Surveillance Ordinance.[xxxi]

Privacy regulation at the local level, which Rubenstein dubs "privacy localism", mitigates two key gaps in federal and state privacy law. The first is related to public surveillance, where there are limited constitutional and statutory protections against government surveillance in public areas. The second gap is associated with fair information practices, which refers to the lack of federal and state privacy laws that apply to local government record-keeping agencies in the collection, use and disclosure of personal information.[xxxii] So-called "sunshine" public records laws are designed to make government open and transparent to members of the public, including through the release of information created by and about smart city technologies.[xxxiii] Indeed, while few local governments in the US are directly impacted by core international frameworks on data management and privacy and federal privacy laws and data governance initiatives, these efforts have raised awareness and expectations about data management and privacy issues at the municipal or local level.

It is important to note that, as the National League of Cities details, "states can preempt cities from legislating on particular issues either by statutory or constitutional law. In some cases, court rulings have forced cities to roll back ordinances already in place."[xxxiv] For example, in Missouri, in 2015, the state supreme court, while not ruling on the legality of the cameras themselves, created a stricter burden of proof that cities must meet if they want to issue red-light traffic tickets.[xxxv] In 2024, New Hampshire voted to ban warrantless police surveillance using facial recognition in the state (HB1688), and while the law applies specifically to state agencies, this means that NH cities cannot use state data that implicates facial recognition.

In designing data collection and management protocols, smart cities can capitalize on robust data frameworks that have already emerged in other sectors and jurisdictions. Key privacy and information governance methodologies and practices including system of records notices (SORNs), records of data processing, data protection impact assessments (DPIAs), data catalogs/inventories, and data-flow diagrams provide vital documentation of permissible purposes for data, alongside knowledge of data lineages and data risks.

As promulgated by the Privacy Act of 1974, system of records notices requires U.S. federal agencies to publish notice of any recordkeeping systems from which information is retrieved by the name of the individual or by some identifier associated with the individual. The notice identifies what information is collected and why, from whom the information is collected, how it is subsequently shared, and how an individual can access and/or correct the record. Written records of processing operations carried out on personal data (required by CCPA and CPRA and Article 30 of GDPR) include information about rationales for data processing, categories of subjects and data processed, data recipients, security measures, and time limits for retention for operational and archival purposes.

Required of US federal agencies and mandated by Article 35 of the EU's GDPR for projects that pose a high risk to personal data, ***data protection/privacy impact assessments (DPIA) are publicly disclosed documents that identify and lay out strategies to mitigate the potential risks associated with collecting, storing, using, and retaining personally identifiable information whether through the adoption of new technologies and/or business processes***. Many privacy laws regulating personal data use and disclosure, including GDPR, CCPA, and CPRA, also require data inventories or something like a data inventory. A data inventory, or record of authority, "identifies personal data as it moves across various systems and thus how data is shared and organized, and its location."[xxxvi]

Cities with stricter surveillance regulations in place now mandate master lists of the city's deployed surveillance tools and annual reports from city departments that use surveillance technology.[xxxvii]

IMPACT ASSESSMENTS

Why camera data is being collected and retained.
- Whether the data is stored, where, and under what conditions.
- What analytics, if any, will be applied to the data.
- Whether attempts to identify individuals in the data will be made systematically or on a case-by-case basis.
- What other information will be combined with the video/image as part of processing.
- Who is authorized to view images and processed data.
- How long images/video will be retained under normal circumstances.
- What measures will be necessary to block or override automated and unauthorized deletion.
- Whether the analytics results are stored directly with the images/video or elsewhere.
- Whether additional privileges are required to access the results of analytics.
- What procedures will be followed to disclose the images/videos to those inside and outside the organization.
- How dissemination rules will be put in place so that they are aligned to retention requirements and that materials are maintained and available for dissemination based on agreements and legally imposed requirements.

The elements of the impact assessment included here are adapted from the U.S. Department of Homeland Security Science and Technology Directorate, Policy Considerations for the Use of Video in Public Safety.

Data Life Cycle Analysis

City functions have always been information-intensive in nature. For example, transportation and public works departments have long designed, developed, and deployed mobility services to the public using maps and plats, planning and zoning records, traffic engineering records, traffic count reports, and accident reports. Emergency management departments have long planned, prepared for, and coordinated around disasters or emergencies utilizing planning studies, emergency operations plans, and incident reports. Local police have long monitored communities and investigated crimes, creating and using case files, criminal history records, and traffic-related records in the process.

Data (in transit and at rest) needs to be managed in ways that plan for and ensure a proper level of control over its lifecycle, with the lifecycle model, in turn, providing opportunities to improve data governance and compliance and minimize liabilities and risks. ***At its most basic, understanding the lifecycle of data involves delineating data types and what happens to that data from creation/generation, to collection, preparation/processing (categorization, organization, transformation, analysis, and visualization), deployment/use, sharing, storage, and disposition.*** In this analysis, data can be demarcated as an asset or a liability depending on the context, with privacy concerns driving data governance policies to address issues of data reduction and removal.

Functions	Activities	Data Types
Transportation Operations	• Traffic management and monitoring (traffic flow - car count/frequency/direction, journey time analysis, optimal bus routes) • Traffic rule violation detection and enforcement (monitoring of reserved lanes, bus lane enforcement) • Parking management (parking lot occupancy detection) • City planning (city modeling, urban-rural classification and planning, corridor mapping)	• Video and image streams • Traffic volumes • Traffic motion (speed, acceleration, stationary duration, crashes) • Turning movement counts (cars, heavy vehicles, pedestrians, motorcycles, bicycles) • Object classification (cars, heavy vehicles, pedestrians, motorcycles, bicycles) • Vehicle classification (license plate, color, category) • Real-time travel trajectory • Travel time • Signal data • Weather data

Table 4. Example of Data Types Associated with Functions and Activities of City Government.

In a lifecycle model, data must be understood in the context of the broader system in which it operates (see Table 4). In the case of smart camera technologies, this includes understanding the sources of video footage or photographs, the software to process captured images for comparison using algorithmic analysis, the server environment, and the databases (containing comparison data sets) against which images can be compared. The latter point speaks to the notion that some services, including biometric identification for facial identification, rely on associating known features with external data sources. Data from these systems is also stored in databases maintained by public and private entities, with policies dictating whether data can be reviewed, shared, transferred, or sold.

In smart city contexts across the US, a model of data stewardship is forming under the direction of Chief Privacy Officers, the efforts of which govern the actions of city agencies, vendors, contractors, and subcontractors. Building a sense of openness and transparency in the data lifecycle happens through formulating written, transparent data policies that are considered by stakeholders. There are various tools that can aid in this process. Data inventories and data maps, in particular, can provide helpful information about electronically stored information's location, type, and ownership. In the process, these tools can be used to investigate critical data dimensions, including the realms of privacy, confidentiality, criticality, ownership, and storage.

When looking to develop or update a policy around records retention, it's crucial to determine whether the data is stored within the system and to identify any associated repositories. Video systems can be designed for real-time viewing only, negating the issue of data storage since no archiving of data is involved. However, in a smart city context video, images, and associated metadata are generally created with the intent that they are captured for some period, whether for single-purpose use or to be archived as historical data. In these instances, data upload, storage, categorization, redaction, access, and deletion are usually handled by operational users using storage and records management systems offered by the vendor community. Such public-private partnerships can complicate how data is controlled and processed with defensible data retention in mind.

The Austin Police Department's body-worn cameras procedure highlights the complexity of such integrations.

"At the end of each shift, officers dock their cameras and all recorded footage automatically uploads to a cloud storage site called Evidence.com. APD cameras do not contain removable storage, so footage cannot be deleted until it is uploaded to the cloud. All footage is classified by officers in conjunction with an automated integration service that captures related data from the dispatch and records management systems. Evidence is retained in accordance with the City retention schedule, and access to video evidence is fully logged. The Austin Police Department provides body-worn camera footage to external agencies by providing a download link from Evidence.com or by directly sharing the footage on an external agency's Evidence.com account. Members of the public who are able to demonstrate that they are an interested party in the recorded incident may request video from APD." [xxxviii]

As a retention tool, a records retention schedule is the policy document that sets out data retention and disposition requirements, including how long data has currency and what happens to the data subsequently - destruction, transfer, expungement, transfer to the archive, etc. The document identifies data at rest (including any categorization of content, e.g., situational awareness data, data to be used as evidence in criminal proceedings), co-located with information related to associated business processes and workflows, and resident within a set repository. However, we note that policies city units and vendors adopt are often invisible to the public.

Traditionally, in determining the length of storage period for recorded video, a balance is generally struck between supporting intended and anticipated operational concerns, aligning with legal requirements (juristically and statutorily imposed, including open records requests), and the rather mundane technical issue of data capacity.[xxxix] Research has found that when discretion is possible, operational retention periods can reflect overall attitudes toward data use. Regarding the retention of body-worn camera data, Fan (2018) found that "while policies tend to be strong on preserving evidence for criminal prosecution, there are gaps regarding preserving evidence for potential civil cases against the department or officers. Moreover, recordings deemed non-evidentiary are stored for a much shorter time before deletion."[xl] As the Brennan Center for Justice notes, "the length of time potential evidence in a court case must be preserved is governed by state law. Retention time for all other video is generally a matter of police policy."[xli]

Newer policy approaches to records retention schedules begin with the premise that retaining personal information in a manner that deviates from legal requirements and/or industry norms requires a clear written business justification. In this instance, current and future operational retention criteria are looked at alongside the legitimate and reasonable needs of stakeholders (including what's in the public interest). Disposition is aligned with relevant compliance frameworks that balance issues of personal privacy and legitimate access for purposes of government accountability and transparency.

It is a truism that "data must exist undeleted to be analyzed" (Fan, 2018).[xlii] Data deletion (particularly as it is implemented following shortened retention periods) serves multiple purposes. It can assure third-party privacy advocates that content is no longer available to be mined, and it can also serve the purposes of those implementing camera technologies by reducing the costs associated with ongoing data storage (Fan, 2018). Yet it is important to note that deleting data, including as part of sanctioned records retention schedules, can be thwarted by technological challenges. At a surveillance technology public comment meeting on April 28, 2023, hosted by the Seattle Police and Information Technology Departments, Captain James Britt discussed the use of hostage negotiation throw phones, devices which include hidden cameras delivering live-feed video for threat and tactical assessments, which can later be uploaded into evidence storage. In this instance, to prevent tampering, the manufacturer set up the system so that the only way to delete individual recordings from the video monitoring console's hard drive (after evidentiary recordings are uploaded to evidence storage via a DVD or USB stick) is by reformatting the entire drive or overwriting the drive when full. It was estimated that given the infrequency of use and the size of the drive it would be several years before recordings (whether in scope or not in scope as evidentiary material) are overwritten.[xliii]

Conclusion

This document provides the reader with frameworks for local government agencies to consider when developing written policies and procedures for deploying surveillance technologies and collecting and retaining data and associated metadata. A holistic view of data from creation forward leads to a more robust conceptualization of the complex issues involved in data collection, retention, and disposition.

Embedding ethics, transparency, and accountability in smart city surveillance technologies means understanding and accommodating privacy concerns while aligning the use of these technologies with legitimate governmental purposes. It means asking why video and other data are being collected and retained, what analytics, if any, will be applied, whether attempts to identify individuals will be made systematically or on a case-by-case basis, and who is authorized to access processed data, among numerous related concerns. It also means considering the impact that surveillance technologies and data policies have on stakeholders and city residents in practice, such as implications for communities that have been historically overpoliced. The four analytical frameworks presented in this white paper can guide ethical decision-making in relation to these issues and concerns when developing smart city policies and procedures.

[i] Electronic Frontier Foundation, *Street-Level Surveillance*, https://www.eff.org/issues/street-level-surveillance

[ii] Douglas MacMillan, "Eyes on the Poor: Cameras, Facial Recognition Watch Over Public Housing," *The Washington Post*, May 16, 2023, https://www.washingtonpost.com/business/2023/05/16/surveillance-cameras-public-housing; Andrew Weber, "Austin Gives Final OK to License Plate Reader Program for Police," *KUT 90.5*, June 9, 2023, https://www.kut.org/crime-justice/2023-06-09/austin-gives-final-ok-to-license-plate-reader-program-for-police; Reuters, "Beijing to Film Building Sites in New Smog Control Measure," April 06, 2014, https://www.reuters.com/article/china-environment/beijing-to-film-building-sites-in-new-smog-control-measure-idINDEEA3604920140407

[iii] Douglas MacMillan, "Eyes on the Poor"; Ira S. Rubinstein, "Privacy Localism," *93 Wash. L. Rev. 1961*, 2018, https://digitalcommons.law.uw.edu/wlr/vol93/iss4/8

[iv] McKinsey Global Institute, "Smart Cities: Digital Solutions for a More Livable Future," 2018, https://www.mckinsey.com/capabilities/operations/our-insights/smart-cities-digital-solutions-for-a-more-livable-future

[v] Shizra Sultan and Christian D. Jensen, "Metadata Based Need-to-know View in Large-Scale Video Surveillance Systems,"*Computers & Security*, *111*, 102452, 2021, https://doi.org/10.1016/j.cose.2021.102452

[vi] San Francisco banned police use of facial recognition in 2019, but reneged on that policy in 2024.

[vii] The directions from the City Council of the City of Austin, for example, have led to recent reductions in license plate data retention from one year to 30 days to 7 days. In these instances, server operators are charged with purging all Automated License Plate Reader (ALPR) data one week after an ALPR collects it. For information on the City of Austin Automated License Plate Reader (ALPR) program, see the Council-Approved Records (including the meeting of June 8, 2023, item 85), available through the Office of the City Clerk: https://services.austintexas.gov/edims/search.cfm

[viii] Add citations to Detroit and SD events

[ix] United Nations, "68% of the World Population Projected to Live in Urban Areas by 2050, Says UN," May 16, 2018, https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html

[x] National League of Cities, *The Future of Equity in Cities*, 2017, https://www.nlc.org/wp-content/uploads/2017/11/Future-of-Equity-in-Cities-2017.pdf

[xi] ProptechOS, *Smart City Index*, 2024, https://proptechos.com/smart-city-index/

[xii] Rob Kitchin, *Digital Timescapes: Technology, Temporality and Society*, John Wiley & Sons, 2023, p. 36.

[xiii] Simon Elias Bibri and John Krogstie, "The Emerging Data–Driven Smart City and Its Innovative Applied Solutions for Sustainability: The Cases of London and Barcelona," *Energy Informatics*, *3*, 7, 2020, https://doi.org/10.1186/s42162-020-00108-6

[xiv] Intel, *Intel® Edge AI Box*, 2024, https://www.intel.com/content/www/us/en/developer/articles/reference-implementation/intel-edge-ai-box.html

[xv] Future of Privacy Forum, "Shedding Light on Smart City Privacy," https://fpf.org/uncategorized/smart-cities/

[xvi] Austin City Charter, "§ 3. - GENERAL POWERS," https://library.municode.com/tx/austin/codes/code_of_ordinances?nodeId=CH

[xvii] Texas Municipal League, *Alphabet Soup: Types of Texas Cities*, 2017, https://www.tml.org/DocumentCenter/View/244/Types-of-Texas-Cities-PDF

[xviii] Rebecca Williams, R., "Everything local surveillance laws are missing in one post," 2021, *Belfer Center for Science and International Affairs, Harvard Kennedy School*. Retrieved from https://www.belfercenter.org/publication/everything-local-surveillance-laws-are-missing-one-post; Margaret Fidler, "Local police surveillance and the administrative Fourth Amendment," 2020 *Santa Clara High Technology Law Journal, 36*(5). Retrieved from https://digitalcommons.law.scu.edu/chtlj/vol36/iss5/2

[xix] An example is the Mobility Management Center (MMC) which functions as the City of Austin's headquarters for monitoring and managing traffic throughout the Austin area.

[xx] U.S. Department of Homeland Security Science and Technology Directorate, *Video Quality in Public Safety (VQiPS): Policy Considerations for the Use of Video in Public Safety*, 2016, p. 14, https://www.dhs.gov/sites/default/files/publications/Policy_Considerations_for_the_Use_of_Video_in_Public_Safety_Final_v5.pdf

[xxi] Gloria J. Miller, "Stakeholder Roles in Artificial Intelligence Projects," *Project Leadership and Society*, *3*, 100068, 2022, https://doi.org/10.1016/j.plas.2022.100068

[xxii] Institute for Local Government, *What Is Public Engagement and Why Should I Do It?*", 2016, https://www.ca-ilg.org/sites/main/files/file-attachments/ilg_what_is_public_engagement_and_why_should_i_do_it_8.31.16.pdf?1472685794

[xxiii] Something about Portland

[xxiv] Teri Figueroa, "San Diego Mayor Orders Smart Streetlights Turned Off," *Government Technology*, September 10, 2020, https://www.govtech.com/public-safety/san-diego-mayor-orders-smart-streetlights-turned-off.html

[xxv] National League of Cities, *A Path Toward Safe and Equitable Cities: Recommendations from the NLC Reimagining Public Safety Task Force*, 2021, https://www.nlc.org/wp-content/uploads/2021/10/nlc-rps-tf-recommendations-report-a-path-toward-safe-and-equitable-cities.pdf

[xxvi] Michael Kwet, "The Rise of Smart Camera Networks, and Why We Should Ban Them," *The Intercept*, January 27, 2020, https://theintercept.com/2020/01/27/surveillance-cctv-smart-camera-networks/; Detroit Community Technology Project, "A Critical Summary of Detroit's Project Green Light and its Greater Context," 2019, June 9, https://detroitcommunitytech.org/?q=content/critical-summary-detroit%E2%80%99s-project-green-light-and-its-greater-context

[xxvii] Mark Schlosberg and Nicole A. Ozer, *Under the Watchful Eye: The Proliferation of Video Surveillance Systems in California*, ACLU of Northern California, 2007, p. 9, https://www.aclunc.org/sites/default/files/under_the_watchful_eye_the_proliferation_of_video_surveillance_systems_in_california_0.pdf

[xxviii] U.S. Department of Homeland Security Science and Technology Directorate, *Video Quality in Public Safety (VQiPS)*, p. 69.

[xxix] Amy Kristin Sanders, Daxton 'Chip' Stewart, and Steven Molchanov, "Is It Just Dumb Luck? The Challenge of Getting Access to Public Records Related to Smart City Technology," 2022, https://www.nfoic.org/wp-content/uploads/2022/10/SmartCities.pdf

[xxx] Nathan Sheard and Adam Schwartz, "The Movement to Ban Government Use of Face Recognition," *Electronic Frontier Foundation*, May 5, 2022, https://www.eff.org/deeplinks/2022/05/movement-ban-government-use-face-recognition

[xxxi] Seattle, *Data Privacy*, https://www.seattle.gov/tech/data-privacy

[xxxii] Ira S. Rubinstein, *Privacy Localism*.

[xxxiii] Amy Kristin Sanders, Daxton 'Chip' Stewart, and Steven Molchanov, "Is It Just Dumb Luck?"

[xxxiv] National League of Cities, *City Rights in an Era of Preemption: A State-by-State Analysis*, *2018 Update*, p. 3. https://www.nlc.org/wp-content/uploads/2017/02/NLC-SML-Preemption-Report-2017-pages.pdf

[xxxv] Collin Reischman, "High Court Knocks Down Red-Light Cameras, *The Missouri Times*, August 19, 2015, https://themissouritimes.com/high-court-knocks-down-red-light-cameras/

[xxxvi] IAPP, "Data Inventory," *Glossary of Privacy Terms*, https://iapp.org/resources/glossary/

[xxxvii] Michael Isaac Stein, Caroline Sinders, and Winnie Yeo, "The Tool Box: A List of the Police Surveillance Tools at the Disposal of the City of New Orleans," *The Lens*, October 21, 2021, https://surveillance.thelensnola.org/toolbox/

[xxxviii] City of Austin, *Austin Police Department Body-Worn Camera Program*, https://www.austintexas.gov/sites/default/files/files/Police/Public_Trn_BWC.pdf

[xxxix] U.S. Department of Homeland Security Science and Technology Directorate, *Video Quality in Public Safety (VQiPS)*.

[xl] Mary D. Fan, "Body Cameras, Big Data, and Police Accountability," *Law & Social Inquiry*, *43*(4), 2018, p. 1237, https://doi.org/10.1111/lsi.12354

[xli] Brennan Center for Justice, "Police Body Camera Policies: Retention and Release," 2019, https://www.brennancenter.org/our-work/research-reports/police-body-camera-policies-retention-and-release

[xlii] Mary D. Fan, "Body Cameras, Big Data, and Police Accountability," p. 1244.

[xliii] City of Seattle Information Technology Department, *SPD Hostage Negotiation Throw Phone Presentation*, 2023, https://www.youtube.com/watch?v=hW3Ty-FBctw