RON GALPERIN
CONTROLLER

July 14, 2021

Honorable Eric Garcetti, Mayor
Honorable Michael Feuer, City Attorney
Honorable Members of the Los Angeles City Council

Re: Protecting Privacy Makes a Smarter L.A.

New technologies present exciting opportunities for local governments to improve the delivery of essential neighborhood services, increase efficiency and enhance the quality of life for residents — making cities more innovative and advanced, and, in turn, "smarter." While Los Angeles continues to pursue smart city initiatives, it is increasingly critical for the City to prioritize the safety and privacy of the Angelenos we serve. This is especially important when it comes to programs that employ surveillance technologies and collect personal data, as they represent serious privacy risks if managed improperly.

The City is currently developing policies and plans to help guide how departments modernize their information services, and how smart technologies are deployed — including the SmartLA 2028 Plan, the Digital Bill of Rights, the Code of Ethics and more. However, at this time, no single City entity is responsible for evaluating the privacy implications created by using surveillance technologies, which often have the ability to analyze the movements, behavior or actions of identifiable individuals. My latest report analyzes the City's privacy-related efforts and recommends a new framework for evaluating and mitigating risks, which will help the City protect residents as it develops new technologies and modernizes services.

A decentralized approach

As it stands, managing information and privacy is typically left to each City department. They must individually determine whether specific technologies or applications are necessary and how these tools will be used to meet their operational needs. My office found that City departments have taken many different approaches to address privacy

risks associated with surveillance tools — an ad hoc method that creates inconsistencies and accountability gaps.

Additionally, the City does not currently define or inventory the surveillance technologies it uses, nor does it designate a responsible body for overseeing departments' use of these tools. While there are some existing data management and security measures in place to ensure that the City's information systems and sensitive records are protected, still lacking is a formal privacy management program that sets specific guidelines for addressing risks associated with the use of surveillance technologies.

Implementing best practices

To ensure the City is adequately protecting the public's privacy, more safeguards are needed and should be consistent with those established by the federal government, the State of California and other local jurisdictions. My report recommends that City policymakers should:

- Clearly **define surveillance technology** and identify what is used by departments.
- Develop a standardized **surveillance impact assessment and reporting** process.
- Establish a **privacy advisory board** to support departments' development of privacy policies and controls.
- Require departments to **update surveillance impact assessments** on an ongoing basis.

As Controller, my goal is to make Los Angeles the smartest, most transparent City in the world. To achieve this, we need to stay up to date with emerging technologies, but at the same time, keep the safety, needs and privacy of Angelenos at the forefront of our work. I urge City leaders to adopt a framework that allows us to evolve and innovate as a City and engender greater public trust in our government.

Respectfully submitted,

RON GALPERIN
L.A. Controller

Protecting Privacy Makes a Smarter L.A.

RON GALPERIN

LA CONTROLLER

Table of Contents

EXECUTIVE SUMMARY

Technology can help governments become more innovative, safer, and even more environmentally friendly. Increasingly, interconnected technologies and systems are facilitating the emergence of "smart cities," which are cities that use technology to collect data, manage assets, increase efficiency, and improve livability and quality of life.

While new technologies present tremendous opportunities to improve the delivery of government services, it is important for the City of Los Angeles to consider how smart technologies that collect, store, and analyze identifiable information, will impact the public's privacy. Balancing these tradeoffs—improved efficiency versus privacy—is critical because without effective and ongoing oversight, these technologies have the potential to encroach on the public's privacy, civil rights, and civil liberties.

This report examines the City's approach to managing privacy risks associated with surveillance technologies, which are tools that track or analyze the movements, behavior, or actions of the public. **We found that while some departments are taking steps to address privacy risks, the City's overall process for evaluating and mitigating risks needs improvement**.

What We Found

The City has developed policies and guidelines intended to promote privacy as it works to modernize information technology services and develop smart city applications, including the City's Privacy Policy, Digital Bill of Rights, Digital Code of Ethics, and Information Security Manual. These and other policies serve as a guide for departments when developing and implementing new solutions, require departments to properly classify sensitive data, and establish standards for information security and access control.

However, it is the responsibility of each department to ensure that surveillance technologies and other information systems adhere to City standards, applicable laws, and privacy best practices. This process sometimes lacks transparency, and there are gaps in how departments identify, evaluate, and mitigate privacy risks. **Based on a review of citywide privacy policies and the privacy management processes of select departments, we found that:**

- **Neither the City's existing codes nor its privacy guidelines define what constitutes surveillance technology, which hinders departments' ability to identify technologies representing elevated privacy risks;**

- **The City does not have an inventory identifying surveillance technologies that departments are currently using, making oversight challenging; and**
- **The City lacks a formal surveillance technology impact assessment process, which can lead to inconsistencies in how departments evaluate privacy risks, develop use policies, and deploy surveillance technologies.**

These weaknesses highlight the need to supplement the City's existing privacy policies, and develop tools that ensure privacy risks are systematically identified and mitigated across all City departments.

What We Recommend

Technology that monitors the activities and movement of the public is not necessarily a bad thing, nor something that should automatically be considered an unreasonable privacy violation, **so long as the need is justified, and effective controls are in place to ensure the public's information is safe from improper use or disclosure.** This report recommends that the City establish a new surveillance impact assessment and management framework.

Specifically, the City should:

- **Clearly define surveillance technology and identify all surveillance technologies used by departments**;
- **Develop a standardized surveillance impact assessment and reporting process**, and post surveillance impact reports on a single City webpage to ensure the public can easily access the information;
- **Establish a privacy advisory board that meets publicly to review surveillance impact assessments**, and oversee departments' development of surveillance technology privacy policies and controls; and
- **Require departments to update surveillance impact assessments** any time a department makes substantial changes to a surveillance system, or how the data from a system will be used, shared, or stored.

By implementing the framework recommended in this report, the City can build trust as it develops and acquires new technologies. These actions will also promote transparency, and allow City leaders, community stakeholders, and members of the public to see exactly how its government is addressing privacy risks, regardless of how smart technologies evolve in the future.

BACKGROUND

New technologies and the emergence of the connected "smart city" present tremendous opportunities for local governments. **Smart cities allow policy makers, public agencies, and local organizations to collaboratively develop integrated programs and applications that can make cities more efficient, and communities better places to live**. New technologies, infrastructure, and partnerships also enable cities to collect and analyze more data than ever before, giving public officials and residents new insights into the issues impacting communities.

Smart technologies are already changing how the City of Los Angeles operates. For example, some City streetlights currently or will soon host smart technologies, including air quality monitoring sensors, electric vehicle charging stations, pedestrian traffic sensors, broadband connectivity, and Wi-Fi. Public safety technology is also changing. The Los Angeles Fire Department (LAFD) has partnered with UC San Diego to develop real-time, predictive wildfire models during wildfire events. The technology, called WIFIRE, uses images from planes, maps, and weather data to predict how fires will spread.

The emergence of new, smarter technologies means that cities are collecting more data about public conditions—and in some cases members of the public—than ever before. Department data highlights how the City of Los Angeles deploys several tools that collect information.

847,077
Hrs. of police body camera footage collected in 2020[1]

499
LAFD drone deployments in 2020

3.6 million
Number of license plate reader scans in 2020[2]

39
Gigabytes of real time traffic data processed daily

11,850
Estimated number of surveillance cameras operated by the City[3]

Notes:
1. Los Angeles Police Department body camera footage only
2. Los Angeles Police Department license plate scans only
3. Estimate primarily includes cameras monitoring public spaces, City facilities open to the public, and Los Angeles Department of Water and Power, Los Angeles World Airports, and Port of Los Angeles assets; it generally does not include cameras that monitor facilities that are closed to the public, such as office buildings, police stations, and jails

While technology innovations and interconnected systems are key in developing smarter and more efficient government, it is critical that the City prioritize the public's privacy as it pursues smart city initiatives. This is especially important for programs or infrastructure that support surveillance technologies, which are capable of collecting or analyzing personally identifiable information, and other forms of potentially sensitive information.

Surveillance Technologies and Tools

Surveillance technologies and tools can generally be defined as those that analyze the movements, behavior, or actions of identifiable individuals in a manner that can reasonably be expected to raise privacy, civil liberties, or freedom of speech concerns. This can include anything from new smart technologies, such as advanced facial recognition software, to more conventional tools, such as security cameras that monitor public spaces.

Monitoring the movement of people and conditions in public spaces can provide valuable data that departments and officials can use to improve the delivery of services, and develop policies that address quality of life, accountability, or even environmental concerns. Law enforcement surveillance tools, such as surveillance cameras, can also play an important role in promoting public safety by deterring criminal activity and supporting criminal investigations.

Some cities are making public surveillance cameras a central part of their public safety strategy. The New York Police Department operates a program known as the Domain Awareness System, which is one of the world's largest networks of cameras, license plate readers, and radiological sensors. The system is designed to detect and prevent terrorist acts, but also provides data for criminal investigations when needed. In 2016, the City of Chicago reported that its Office of Emergency Management and Communication managed a network of more than 27,000 public and private sector surveillance cameras, while the City of Atlanta manages a network of more than 10,000 publicly and privately-owned cameras.

Examples of how local governments use surveillance tools for law enforcement and non-law enforcement purposes are highlighted below.

Law Enforcement	Non-Law Enforcement
Cameras *mounted on helicopters, drones, vehicles, and officers help public safety agencies monitor incidents in real time, and record employees' interactions with the public.*	***Traffic cameras and sensors*** *let transportation agencies monitor traffic flows, patterns, and congestion, and then make real-time adjustments to traffic lights or other traffic control tools.*
Public safety surveillance cameras *mounted in public spaces allow police agencies to monitor public spaces, collect evidence, and deploy resources when necessary.*	***Unmanned aerial vehicles (UAVs)****, better known as drones, allow fire departments, municipal utilities, and other agencies to evaluate fire and infrastructure risks from multiple vantage points.*

Law Enforcement	Non-Law Enforcement
Automated license plate readers (ALPR) *capture images of license plates, automatically recognize license plate numbers, and can store and compare them to "hot lists."*	***Amperage testing devices*** *allow municipal utilities to measure the amount of electricity consumed at a site, and determine whether an individual is diverting an electrical current.*
Predictive analytics software *allows law enforcement agencies to analyze multiple complex data sets to identify trends and relationships, and predict public safety risks.*	***Remote-operated hazmat response and firefighting vehicles*** *allow public safety personnel to evaluate and mitigate dangerous conditions from a safe distance.*

The City of Los Angeles does not necessarily use all of these surveillance tools. For example, the Los Angeles Police Department (LAPD) does manage an ALPR program, but does not currently use predictive analytics applications for policing.

As the City of Los Angeles, like many of its peers, continues to implement new technologies with surveillance capabilities, it must ensure departments collect, analyze, and safeguard data about members of the public in a responsible and ethical manner.

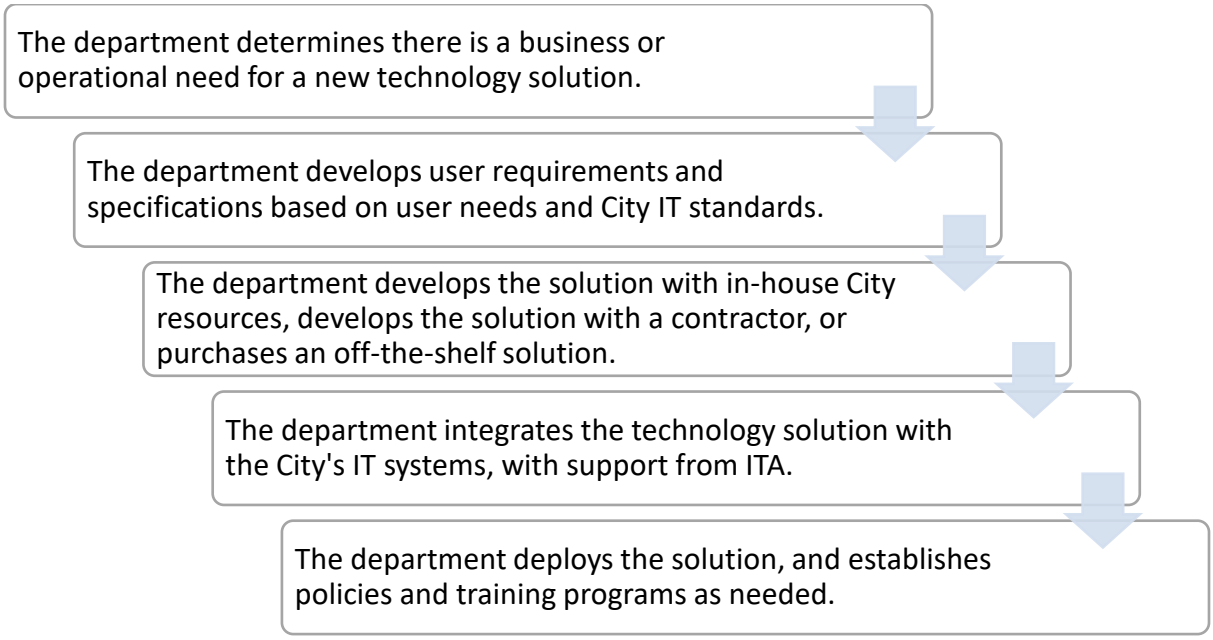
I. The City's Approach to Surveillance and Privacy

Managing information technology resources across an organization as large as the City of Los Angeles presents challenges. The manner in which City departments manage smart technologies and surveillance tools varies. There are several stakeholders within the City that can weigh in on how to best manage these tools, **but no single body is responsible for evaluating the privacy implications and needed safeguards for surveillance technology used by departments.**

Departments Are Ultimately Responsible for the Development of Technology Programs Based on Their Operational Needs

Management of the City's information technology systems and resources, and the data that these systems collect and sometimes store, is a joint effort between departments that "own" a system and are the end-user, and the Information Technology Agency (ITA), which coordinates the implementation and management of the City's technology and digital services. **However, it is usually the responsibility of each department to determine whether specific technologies or applications are needed, and how the tools will be used.**

The typical process for developing or acquiring a technology solution is described in the summary chart below. It is important to note that this process can vary based on the type of technology, the scope and cost of the project, and department procurement policies.



Other offices and departments are also involved in the technology development process when a department chooses to work with external vendors. The Office of the City Attorney for example reviews all contracts, while the City Administrative Officer reviews department justifications for contracts.

Citywide Information Technology and Privacy Policies

The City's information technology and privacy policies have been established by ITA, the Office of the Mayor, and the Information Technology Policy Committee (ITPC). The ITPC, which is composed of information technology specialists from across the City, works closely with ITA and serves as a steering committee and rulemaking body that develops citywide IT policies.

The City has developed several policies that reflect City efforts to modernize information services, improve residents' access to digital services, and promote privacy. Summarized below are key policies and guidelines.

Policy / Guideline	Summary
City of LA Privacy Policy	*Defines the City's rules and responsibilities with regard to collecting and storing personally identifiable information.*
City of LA Digital Bill of Rights*	*Establishes eight privacy rights and safeguards for Angelenos, including the right to privacy, the right to exclusive ownership of personal data, and the right to full disclosure and transparency.*
City of LA Digital Code of Ethics*	*Contains ten "digital standards" designed to be a practical guide for departments when developing policies for emerging technologies, including artificial intelligence, predictive analytics, chatbots, drones, facial recognition technologies, and sensors.*
Information Classification Policy	*Requires departments to properly classify sensitive data (health information, credit card data, PII, etc.), and provides instructions on how each type of information shall be stored, guarded, and transmitted.*
Executive Directive 2 – Cybersecurity	*A Garcetti Administration policy to make City systems more resistant to attacks and penetration; establishes a series of minimum IT security standards to be followed by all departments and creates the Cyber Intrusion Command Center.*
Information Security Manual	*Serves as the City's cybersecurity policy and manual; outlines responsibilities and expectations for the security, access control, systems acquisition, and management of the City's digital and information assets.*

*Pending final publication

While these and other policies serve as important information security and management guidelines for all departments, policy and accountability gaps may result in departments failing to address privacy risks posed by certain technologies.

Transparency, Approvals, and Oversight for City Surveillance Technologies Can Be Inconsistent

The City's existing data management and information security policies are critical to ensuring information systems and sensitive records are protected. However, these controls do not always address when it is appropriate to collect information about members of the public without their knowledge, nor do they establish oversight and transparency measures that

ensure departments minimize the risk of sensitive data being inappropriately accessed, used, or shared.

The City does not currently define surveillance technology, nor does it designate any particular official or body as responsible for monitoring City departments' use of surveillance tools, and other systems that may impact the public's privacy. **This also means the City does not have a single inventory identifying surveillance technologies deployed by departments**. Generally, it is the responsibility of each department to:

- Determine when technology that could be considered a surveillance system is needed;
- Develop or acquire the system, software, or equipment;
- Develop policies and procedures governing use of the technology and any data that is collected or retained; and
- In conjunction with the City Attorney's Office, ensure the technology is used in accordance with applicable federal, state, and local regulations.

Without specific guidelines for managing privacy risks associated with surveillance technology, departments must develop such programs and evaluate privacy implications on an ad-hoc basis. Those evaluations might also vary based on the instructions provided by a department's governing board, such as the Board of Police Commissioners or the Fire Commission.

Department Efforts to Evaluate and Mitigate Privacy Concerns

The lack of a defined privacy management program for City surveillance technologies creates challenges for departments, and hinders City efforts to promote transparency. It also results in policy gaps, as City departments often differ in how they identify, analyze, and address privacy concerns when developing programs that will impact the public's privacy.

For example, in February 2020 the California State Auditor issued a report highlighting several weaknesses in the Los Angeles Police Department's (LAPD) management of its ALPR program. The audit, which focused on use of ALPR systems by local law enforcement agencies, found that while the LAPD did publish documents describing their ALPR systems, the department did not have an ALPR privacy policy, as required by state law. Auditors also found LAPD's user access controls to be insufficient, as all computers assigned to staff, regardless of the employee's position, included ALPR software. There were approximately 13,000 employees with ALPR system access at the time of the audit.

According to the LAPD Office of Constitutional Policing and Policy, the department has since addressed the issues identified by the State Auditor and is in full compliance with State law.

However, the State Auditor's findings highlight the need for a standardized process that supports departments' efforts to mitigate privacy risks posed by new technologies.

Overall, City departments have taken different approaches to address privacy risks associated with surveillance tools. The chart below provides a high-level summary showing the steps select departments, including LAFD, the Department of Transportation (LADOT), LAPD, and the Bureau of Street Lighting (BSL), have taken to address surveillance technology privacy risks. It is important to note that departments are not necessarily required to complete all of the following privacy assessments when developing a new program, nor are they required to obtain all of the approvals listed below.

	LAFD Unmanned Aerial Vehicles	**LADOT** Automated License Plate Readers	**LAPD** Public Safety Surveillance Cameras[1]	**LAPD** Helicopter Camera Recording[2]	**BSL** Streetlight Surveillance Cameras Pilot[3]
Implemented	**2017**	**2016**	**2007**	**2020**	**2021**
Primary purpose	Emergency response	Parking enforcement	Investigations	Situational awareness	Monitor smart nodes / copper wire theft
Consulted the City Attorney's Office	✓	✓	✓	–	–
Conducted a formal privacy assessment	✓	✓	–	–	–
Consulted outside subject matter or privacy experts	✓	–	✓	–	–
Use and data management policy in place	✓	✓	✓	✓	–
Use approved by dept governing board	✓	–	–	✓	–
Use approved by the City Council	✓	✓	✓	–	–

Notes:
1. Applies to the Gang and Narcotics Division surveillance cameras mounted in public spaces
2. While helicopter-mounted surveillance cameras have been in use for more than 20 years, video footage recording and download capabilities were implemented in November 2020
3. BSL noted this is a limited pilot program that may be formalized following the testing / pilot phase

Inconsistencies in the rollouts of systems and tools with surveillance capabilities highlight the need to supplement the City's existing privacy policies, and develop a program that provides policymakers and City officials with the information necessary to systematically identify and mitigate privacy risks. Opportunities also exist to make this process more transparent.

II. Lessons from Other Government Entities

Federal agencies, State of California agencies, and several local governments offer lessons in balancing the need to collect information about the public with the need to protect individuals' civil liberties and fundamental privacy rights. These government entities have implemented technology procurement and management rules specifically designed to address privacy concerns.

Federal and State Strategies

Section 208 of the E-Government Act of 2002 requires all federal government agencies that develop or procure new technology involving the collection, management, or dissemination of personally identifiable information to perform comprehensive Privacy Impact Assessments. Federal agencies must show that system owners have incorporated privacy protections throughout the entire lifecycle of a system. The Privacy Impact Assessments must be made publicly available, with some security and competitive business interest exceptions. The law also applies when agencies make substantial changes to existing systems.

State of California agencies are also required to complete privacy assessments similar to those performed by the federal government. State Administrative Manual Section 5310.8 requires information asset owners to conduct a baseline Privacy Threshold Assessment, and if necessary, a comprehensive Privacy Impact Assessment, upon acquiring, developing, or making changes to an information system. Privacy Threshold Assessments enable departments to analyze at a high level whether systems will collect, maintain or share private information, such as names, dates of birth, health information, biometric information, physical descriptions, education or employment histories, and license plate data, among other forms of data.

Should a department determine, based on a Privacy Threshold Assessment, that an information system will have an effect on a person's privacy, it must then perform a Privacy Impact Assessment. When completing a Privacy Impact Assessments, an agency must identify privacy risks associated with the system, and describe steps it will take to mitigate those privacy risks.

Steps Taken by Other Cities

There are also several local governments that have taken proactive steps to identify and assess technologies that represent a privacy risk. **Cities such as New York, Seattle, and Oakland are all examples of jurisdictions that have passed laws establishing standardized privacy evaluation processes for surveillance technologies**. All three cities require departments to identify technologies that are used for surveillance purposes, and conduct formal surveillance impact assessments. The City of New York's law covers only technologies used by its police department.

In addition to formal surveillance impact assessments, Seattle and Oakland both require additional layers of review and approval. Seattle and Oakland require departments to submit surveillance privacy assessments to a privacy advisory council. The privacy advisory councils, which meet publicly to allow for public comments, evaluate the privacy assessments and recommend additional privacy safeguards as needed. Seattle and Oakland also require city council approval prior to departments deploying surveillance technology, and both cities have worked to retroactively evaluate existing surveillance technologies as well.

III. Managing the City's Privacy Risks Moving Forward

The City's inconsistent approach to managing surveillance technologies stands in contrast to privacy efforts by the federal government, State of California, and other local jurisdictions. These oversight gaps can have negative consequences and foster public distrust. To ensure City departments are adequately protecting the public's privacy, additional safeguards are needed.

Recommendation

The City Council should request that the City Legislative Analyst, with assistance from the City Attorney and City Administrative Officer as needed, develop a proposal for the establishment of a new surveillance privacy review process. The proposal should specifically consider implementation of the best practices listed below.

Clearly define surveillance technology and identify surveillance technologies used by departments

Clearly defining surveillance technology is necessary in order to identify systems and equipment that monitor the movement and activities of the public, regardless of whether the information is collected for law enforcement or non-law enforcement purposes. This definition would guide departments in identifying surveillance technologies already in use, and help them determine whether technology initiatives in the future will require in-depth privacy analysis.

Develop a standardized surveillance impact assessment and reporting process

The City should develop a standardized surveillance impact assessment procedure to ensure the City systematically, and consistently vets privacy issues associated with surveillance technology. This would mean that any department planning to introduce a surveillance tool would need to evaluate the program against a standardized set of privacy considerations, and issue a report, prior to deploying the tool. The process should also apply retroactively to existing surveillance tools, and in rare cases where a department must deploy a surveillance tool for public safety reasons prior to completing a privacy impact assessment.

At a minimum, departments would need to (1) describe the technology and how it will be used, (2) justify the need for the technology, (3) specify whether the technology is subject to any laws or regulations, (4) describe steps the department will take to minimize privacy risks, and (5) present a policy addressing the technology's use, and data management, access, sharing, and retention protocols. All surveillance impact reports should be posted on a single City webpage to ensure the public can easily access the information.

Establish a privacy advisory board to support departments' development of surveillance technology privacy policies and controls

Given the unique and constantly evolving privacy implications associated with the development of smart cities, the City should establish a privacy advisory board. The group, which could consist of outside experts, experts from within the City, or a combination of both, would evaluate departments' surveillance impact reports. Importantly, this advisory board would review the reports during public meetings, allowing members of the public and community organizations to provide input, and outline reasons for supporting or objecting to any elements of a department's plan.

Specifically, the board would evaluate whether use of the application or tool is adequately justified, and whether department policies are adequate to safeguard the information collected by the technology. If necessary, the board would recommend additional privacy controls. The review board could also recommend that the use of certain technologies, if particularly sensitive or controversial, be reviewed by the City Council.

Require departments to update surveillance impact assessments on an ongoing basis

Evaluations of the City's surveillance tools should evolve as those technologies, or the application of those technologies, change. Departments should update surveillance impact assessments any time a department enhances or makes substantial changes to a surveillance system, or how the data from a system will be used, shared, or stored. This will ensure that City executives, policymakers, and the public are aware of significant program changes.

Conclusion

The emergence of smart, interconnected cities offers tremendous opportunities for innovation and efficiency. However, as the City collects and analyzes more data, it must be transparent, and continuously examine how new and emerging technologies will impact the public's privacy. By implementing the privacy framework recommended in this report, City leaders, community stakeholders, and members of the public can be confident that departments are safeguarding private information, and mitigating pressing privacy risks as technology evolves.

RECOMMENDATION TABLE

Number	Recommendation
Responsible Entity: City Council	
1	The City Council should request that the City Legislative Analyst, with assistance from the City Attorney and City Administrative Officer as needed, develop a proposal for the establishment of a new surveillance privacy review process. The proposal should specifically consider: a. A definition for surveillance technologies; b. Development of a standardized surveillance impact assessment and reporting process for existing and future surveillance technologies deployed by departments; c. Establishment of an advisory board to review the impact of City surveillance technologies, privacy risks, and department policies and protocols for mitigating those risks; and d. Requirements for departments to update surveillance impact assessments on an ongoing basis.