Surveillance Annual Report

2020

San Francisco Bay Area Rapid Transit District

Revision 1.1

Executive Summary

2020 Surveillance Annual Report

Pursuant to the District's surveillance ordinance, staff must bring an annual report to the Board regarding the use of approved surveillance technologies and request approval for continued use of those technologies. This report is intended to allow the Board of Directors an opportunity to determine whether the benefits to the community of the surveillance technologies implemented outweigh the costs, and that civil liberties and civil rights are safeguarded.

The Bay Area Rapid Transit District's Annual Surveillance Report covers the initial time period through June 30, 2020 and includes all surveillance technology previously approved by the Board. It is important to note that BART has taken a community based and collaborative approach with regards to policy development and implementation of surveillance technology. All the surveillance technology deployed at BART has the sole goal of improving public safety and security, or otherwise enhancing public trust and the communities experience at BART. This is reflected in the entire process of surveillance technology proposal through policy development and implementation of technology. Each technology must go through several steps before being presented to the BART Board of Directors for approval and implementation.

There are several guiding principles with respect to the use of District approved surveillance technology. First and foremost is the inherent principle that the decision to use surveillance technology should balance security and privacy interests, and shall not be used to harass, intimidate, or discriminate against any individual or group and further, the technology shall not be used for immigration enforcement actions. Additionally, the program must have robust controls in place to prevent the release or misuse of the data collected.

A key success in BART's implementation of its Surveillance Program has been community collaboration. In each area of surveillance technology packages that were presented and approved by BART's Board of Directors; transparency and outreach to the both the community and privacy groups was vital in understanding the concerns

expressed by the community as to how the technology would be used and the data protected. BART met with key community partners, such as Oakland Privacy and Secure Justice to understand the privacy concerns and ensure protective measures are put in place to prevent release or misuse of data collected by the technologies.

Per the San Francisco Bay Area Rapid Transit District's Code of Ordinances, this **Surveillance Annual Report** is a written report concerning the specific surveillance technology in active use by the District. Per Ord. No. 2018-1, this report includes all of the following for the 7 Board approved surveillance technologies:

a) A reasonably specific description of **how the surveillance technology was used**;

b) Whether and **how often data acquired through the use of the surveillance technology was shared** with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);

c) A **summary of community complaints** or concerns received by the BART District related to the surveillance technology;

d) The **results of any internal audits**, any information about violations of the Surveillance Use Policy, and any actions taken in response;

e) Information, including **crime statistics**, if the equipment is used to deter or detect criminal activity, that help the community assess whether the surveillance technology has been effective at achieving its identified purposes;

f) Statistics and information about **public records act requests** related to surveillance technology; and

g) Total **annual costs** for the new surveillance technology, including personnel and other ongoing cost.

Table of Contents

2020 Surveillance Annual Report

Contents

Approved Surveillance Use Policies

At the time of this report, the following Surveillance Technologies have been approved by the Board:

1. **BART Closed Circuit Television**
   Department: Maintenance & Engineering
   ID Number: ME-BCCTV-SUP-01
   Board Approved: October 2018
2. **BART CCTV Public Video Monitors**
   Department: Maintenance & Engineering
   ID Number: ME-BCCTVPVM-SUP-01
   Board Approved: October 2018
3. **BART Public Emergency Phone Towers**
   Department: Maintenance & Engineering
   ID Number: ME-BPEPT-SUP-01
   Board Approved: October 2018
4. **BART Mobile Applications & Related Modifications to BART.gov**
   Department: Office of the Chief Information Officer
   ID Number: OCIO-BMAARMTB-SUP-01
   Board Approved: October 2018
5. **BART Automated License Plate Recognition (ALPR)**
   Department: BART Police Department
   ID Number: BPD-ALPR-SUP-02
   Board Approved: April 2019
6. **BART Research Data Collection and Usage**
   Department: Marketing & Research
   ID Number: OEA-BMRDDCU-SUP-06
   Board Approved: March 2019
7. **BART Trip Verification Technology**
   Department: Planning & Development
   ID Number: PD-TVD-SUP-01
   Board Approved: October 2019

1. BART Closed Circuit Television

2020 Surveillance Annual Report

Surveillance Technology Use

Description: The use of cameras based on closed-circuit television (CCTV) technology to increase the confidence of the community in public transportation and improve the protection of patrons, employees, railcars, and critical infrastructure. The authorized use includes constant facility surveillance, 24 hours a day, 7 days per week within all San Francisco Bay Area Rapid Transit District properties. The cameras are not used in areas where there is a reasonable expectation of privacy, such as restrooms. CCTV data provides critical situational awareness for Transportation and Operations Control Center staff for managing busy stations and special events. Information provided by CCTV systems also reduce delays in revenue service by allowing BART personnel to avoid train-holds in situations that can be resolved remotely by CCTV. CCTV data is also used for accident/incident investigations, mechanical failure investigations, and CPUC compliance checks.

Surveillance technology within the BART system has proven to be a vital resource for police criminal investigations. In order to meet the burden of proof, "beyond a reasonable doubt", every District Attorney's office the BART Police Department interacts with has routinely based their decision to file a criminal complaint based on the availability of quality surveillance video. CCTV footage has provided vital pieces of direct evidence in several homicides and other investigations of violent crimes and has led to the identification and capture of multiple perpetrators. BART Police detectives use surveillance videos on a daily basis to solve a variety of crimes against property and crimes against persons.

Data Sharing

The BART CCTV system is deployed on a secure network that is segmented and isolated from other network traffic. Access to the CCTV network for BART employees is limited to a need to know, right to know basis and no direct access is provided to any persons or organizations outside of BART, other than providing copies of video evidence as

required by subpoena, judicial order, other legal obligation, or to assist with criminal investigations by law enforcement agencies in compliance with the District's Safe Transit Policy. The following tables provide a summary of the recipients of CCTV video recordings during FY20;

Sources of CCTV Requests	
BART PD Investigations	3,723
Internal BART Requests (Not Law Enforcement)	180
Court Subpoenas	33
California Public Request Act	118
Outside Law Enforcement Requests	198
Total CCTV Requests	**4,252**

Outside Law Enforcement Agencies Receiving CCTV Data		
Alameda County Sheriff's Office	Dublin PD	Richmond PD
Contra Costa County Sheriff's Office	El Cerrito PD	San Bruno PD
San Mateo County Sheriff's Office	East Bay Regional Parks PD	San Francisco PD
Alameda PD	FBI	San Leandro PD
Antioch PD	Fremont PD	San Francisco Department of Police Accountability
Berkeley PD	Hayward PD	Union City PD
Broadmoor PD	Human Services Agency	Alameda County DA
Colma PD	Oakland PD	Contra Costa County DA
Concord PD	Oakland Housing Authority PD	San Mateo County DA
California Highway Patrol	Pittsburg PD	San Francisco County DA
Daly City PD	Pleasanton PD	

Complaints

BART customer service has received 15 complaints from passengers who feel that there is insufficient CCTV coverage in the BART system.

Surveillance Policy Compliance

There were no violations of the Surveillance Use Policy for the CCTV system discovered during this period. A random audit of CCTV video requests was conducted for policy compliance. The audit examined 50 randomly selected cases which were handled by

the video recovery unit to determine if the video was provided in compliance with the CCTV Surveillance Policy. The video requests included law enforcement investigations and non-criminal requests. All records examined were found to be in compliance with the policy.

Crime Statistics

Video surveillance is essential for the effective operation of a public transit system. CCTV data provides critical situational awareness for the Operations Control Center for managing busy stations and special events. Information provided by CCTV systems also reduce delays in revenue service by allowing BART personnel to avoid train-holds in situations that can be resolved remotely by CCTV. CCTV data is also used for accident/incident investigations, mechanical failure investigations, and CPUC compliance checks. Aside from the operational uses, one of the primary public safety benefits of a robust CCTV system is the deterrent effect that is provided by the presence of cameras monitoring public spaces. CCTV footage also provides critical information for civil cases and accident investigations. The presence of the CCTV cameras pre-dates the Surveillance Ordinance by several decades. BART stations have always been commissioned with CCTV cameras already in place, making a before/after comparison based on crime statistics impossible. However, there are numerous incidents every year at BART where CCTV evidence provides critical information to solve a crime or identify suspects. During the period of this report, BART Police detectives produced over 400 wanted persons bulletins using CCTV images to attempt to identify persons involved in criminal activity. And of the 4,252 requests for police video, 3,954 of the requests were for criminal investigations or court subpoenas. A matrix showing the breakdown of video requests is provided under Data Sharing section for this technology.

Use of the CCTV surveillance technology within the BART system has proven to be a vital resource for police criminal investigations. In order to meet the burden of proof, “beyond a reasonable doubt”, every District Attorney’s office the BART Police Department interacts with has routinely based their decision to file a criminal complaint based on the availability of quality surveillance video. While data is not currently collected to track cases that were charged because of the availability of CCTV

video, many District Attorneys will not charge cases lacking video evidence. CCTV footage has provided vital pieces of direct evidence in several homicides and other investigations of violent crimes and has led to the identification and capture of multiple perpetrators. BART Police detectives use surveillance videos daily to solve a variety of crimes against property and crimes against persons.

Establishing a causal relationship between the occurrence of crime and the presence, or absence, of CCTV is beyond the scope of this report, but CCTV is an essential part of the safety and security strategy that customers and employees expect the District to provide as part of running a Tier-I mass transit system.

Crime statistics are published monthly and are available at;
https://www.bart.gov/about/police/reports
https://www.crimemapping.com/map/agency/454

Public Records Act Requests

There were 118 public records act requests for video footage, there were no public records requests located which were associated with the CCTV technology itself.

Costs

4,252 individual requests for video evidence were processed by the BART Police Video Recovery Unit in FY20. Processing the volume of video requests requires 4 FTE's assigned to the unit. There were 440 requests for train car video evidence processed by the staff assigned to RS&S.

Overall, the maintenance and operational cost for the 4,563 CCTV cameras operational on train cars (including video recovery from the cameras) in FY20 was approximately $270,000.

The cost to maintain the 3,570 CCTV cameras, including supporting network and data-center infrastructure, deployed in facilities across the BART system (not including train cars) in FY20 was approximately $2,250,000. The cost includes maintenance of CCTV

equipment in non-public areas of the BART system that are not covered by the Surveillance Ordinance.

The primary purpose of the CCTV system in stations is for operational needs outside of law enforcement and the ongoing maintenance costs associated with CCTV systems would continue regardless of whether the system was utilized by law enforcement.

2. BART CCTV Public Video Monitors

2020 Surveillance Annual Report

Surveillance Technology Use

Description: The CCTV Public Video Monitors are deployed above two entry fare gate arrays at Civic Center BART Station. The locations of the monitors were jointly determined by the BART Police Department and BART Operations to deter fare evasion and reduce crime in these areas by alerting the public that a CCTV system is operating in these areas. Authorized use includes public information and awareness that CCTV surveillance is in the BART stations.

Data Sharing

The CCTV Public Monitors are a passive display only device, no recording capabilities exist. Any person in proximity to the display may view the images on the screen which are live streamed from selected CCTV cameras in the area.

Complaints

There were no complaints received for the CCTV Public Video Monitors.

Surveillance Policy Compliance

There were no violations of the Surveillance Use Policy for the CCTV Public Video Monitors discovered during this period. No audit was conducted during this initial reporting period.

Crime Statistics

The CCTV Public Monitors were installed at Civic Center Station as part of the District's efforts to reduce fare evasion. While specific crime statistics associated with the monitors were not analyzed for this report, the feedback from frontline employees was that the monitors were not effective, and the test is therefore being discontinued.

Public Records Act Requests

There were no public records act requests for the CCTV Public Video Monitors.

Costs

Beyond the installation costs for the Board approved project, there were no ongoing maintenance and operational expenses. This project is being discontinued and the monitors will be converted to elevator-status information displays.

3. BART Public Emergency Phone Towers

2020 Surveillance Annual Report

Surveillance Technology Use

Description: The primary use for the Public Emergency Phone Towers is to provide a direct connection to the BART Police Integrated Security Response Center for BART passengers and employees to report emergencies or unsafe conditions. Under the approved project, the Public Emergency Phone Towers were deployed at the Coliseum BART station as a testbed. A full deployment throughout the District would require 204 units on 69 station platforms, although no further installations are planned at this time. The design specifications call for three units per platform evenly distributed for maximum effectiveness. These towers are equipped with emergency phones, blue strobe lights, and surveillance cameras. Where installed, the Public Emergency Phone Towers are available 24 hours a day, 7 days per week. The Public Emergency Phone Towers provide a quick and simple way for BART passengers and employees to alert BART Police that emergency assistance is needed while also providing additional platform CCTV surveillance.

Data Sharing

The Public Emergency Phone Towers include CCTV cameras which are part of the larger CCTV surveillance system. Use of the CCTV camera footage from the Public Emergency Phone Towers is controlled by the CCTV Surveillance Policy. See data sharing for Item 1 – BART Closed Circuit Television for details of data sharing for CCTV data. No data is shared from the Public Emergency Phone Towers other than CCTV footage recorded by the included cameras.

Complaints

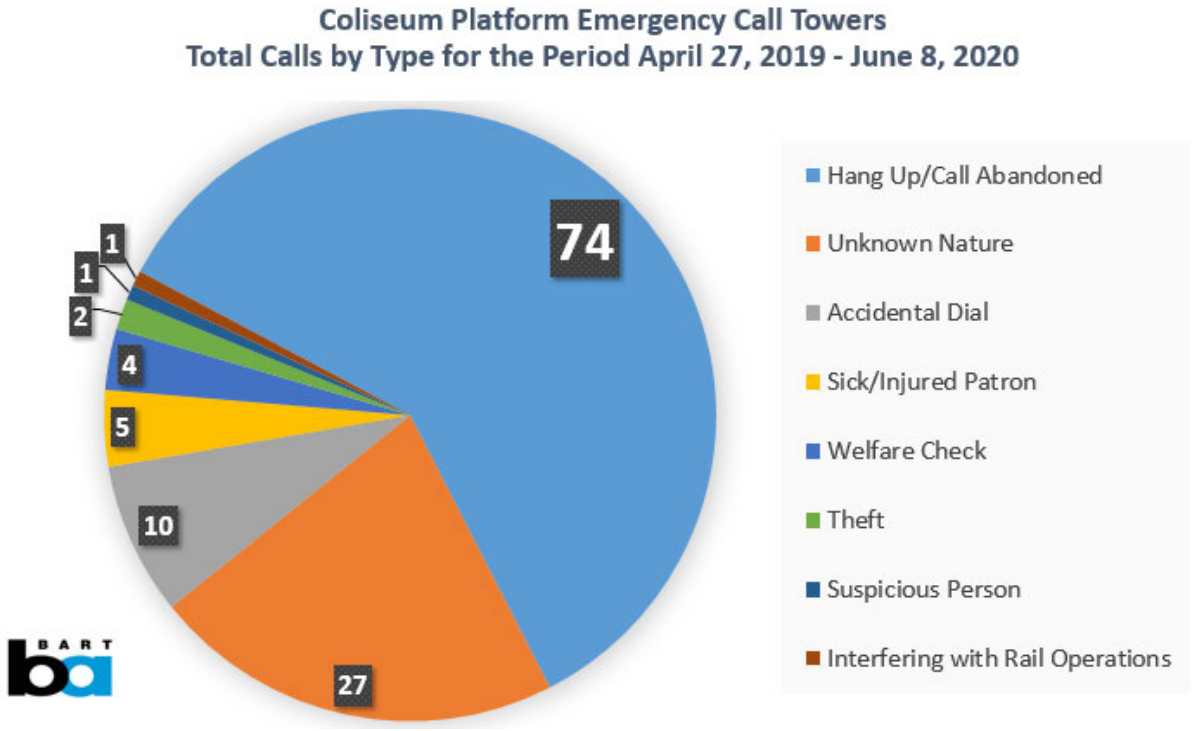
There were no complaints received for the Public Emergency Phone Towers.

Surveillance Policy Compliance

There were no violations of the Surveillance Use Policy for the Public Emergency Phone Towers discovered during this period. A random audit of CCTV video requests was conducted for policy compliance which covers the same CCTV system used by the Public Emergency Phone Towers. See Surveillance Policy Compliance for Item 1 – BART Closed Circuit Television for details of the audit.

Crime Statistics

The following chart reflects the usage of the Public Emergency Phone Towers at the Coliseum Station.



Additional crime statistics are published monthly and are available at;
https://www.bart.gov/about/police/reports
https://www.crimemapping.com/map/agency/454

Public Records Act Requests

There were no public records act requests located for the Public Emergency Phone Towers.

Costs

Beyond the installation costs for the Board approved project, ongoing maintenance will require 4-hours of labor every 30-days totaling approximately $3,600 per year.

4. BART Mobile Applications & Related Modifications to BART.gov

2020 Surveillance Annual Report

Surveillance Technology Use

Description: The primary use for this technology is to provide consistent transit information, transit incentives and maps to BART riders through BART.gov and BART Mobile apps, collectively referred to as "BART Applications". These BART Applications are also used to handle financial transactions, provide proof of payment, and aide the BART Police Department in payment and carpool enforcement. Authorized use includes Navigation, Trip Planning, Fares, Parking, Bike Storage Transactions, Transaction Enforcement, Transit System Analysis & Demand Management, Providing & Redeeming Incentives, Transit Information & Communication, and Surveys.

Data Sharing

The following Authorized BART Service Providers provide elements of support, and infrastructure related to the ongoing operation of the BART Mobile Applications & Related Modifications to BART.gov:

Authorized BART Service Providers		
Hacon	TransSight	Amazon Web Services
Moovel	Auth0	Salesforce Service Cloud
PayPal/Braintree	Acquia	Salesforce Marketing Cloud

Complaints

There were no complaints received for the BART Mobile Applications & Related Modifications to BART.gov.

Surveillance Policy Compliance

There were no violations of the Surveillance Use Policy for the BART Mobile Applications & Related Modifications to BART.gov discovered during this period. Although no audit was conducted during this initial reporting period, it should be noted

that we have mechanisms of continuous monitoring for additions of administrative access, activity logging, firewalling, intrusion detection, and intrusion prevention which may be used for future audits.

Crime Statistics

Implementation of parking features on the mobile application is supporting more robust and efficient enforcement of BART's parking rules, such as automating carpool validation and checking that those paying for parking are using BART. When the carpool user enters BART, the system automatically checks to make sure they and their carpool partner entered within a twenty (20) minute window.

Public Records Act Requests

There were no public records act requests for the BART Mobile Applications & Related Modifications to BART.gov.

Costs

Beyond the installation costs of $1.76M for the Board approved project, the actual ongoing maintenance and operational expenses related to this surveillance technology are $622,000 per year.

5. BART Automated License Plate Recognition (ALPR)

2020 Surveillance Annual Report

Surveillance Technology Use

Description: The goal of installing Automated License Plate Recognition (ALPR) technology is to improve the safety and protection of BART patrons, employees and their vehicles while in BART owned and or operated parking areas and garages. The Use Policy and Impact Reports were drafted in early January 2019 and updated in October 2019. The Impact and Use Reports were produced as collaborative effort with key privacy groups such as Oakland Privacy and Secure Justice. The collaborative nature of this effort allowed for a transparent and robust policy that met all elements of BART's Surveillance Ordinance and California Civil Code Sections 1798.90.51 and 1798.90.53. Over a four-month period from January to April 2019 BART Police met with Privacy Groups to understand privacy concerns and put in place protective measures to prevent misuse of data aired by the ALPR. The ALPR project was approved by the BART Board of Directors for a pilot program on 25 April 2019 for a single installation at Macarthur Parking Garage. This location was chosen because of the high numbers of parking related crimes in the parking garage as well as having existing electronic and structural infrastructure that was already in place in the garage. Since the existing wiring and mounting infrastructure was in place at Macarthur Parking Garage, it made sense to install the cameras at this garage with the goal to see if it made a positive impact in reducing crime in the parking garage prior to making a larger capital investment for installing additional cameras.

Additionally, ALPR has been approved to assist with the efficient enforcement of parking program compliance through the automated enforcement of BART's parking rules. Using ALPR for parking enforcement improves compliance with parking rules, provides documentation support for complaint resolution, and can increase customer satisfaction by providing improved data on space availability. The proposed use of ALPR for parking enforcement has not yet been implemented.

Data Sharing

Following the BART ALPR project approval, the next steps included establishing and ensuring the security of the data collected by the BART Police ALPR system. The Board approved project transmits the data to a secure location at the Northern California Regional Intelligence Center (NCRIC) where physical access is limited to authorized individuals and involves significant physical access protections and digital firewalls.

A Memorandum of Understanding and Agreement (MOU) was signed between the BART Police Department and the NCRIC on October 23, 2019. It should be noted that while signatories of the MOU were between the two agencies, privacy groups such as Oakland Privacy and Secure Justice were also involved in the development of this document to ensure transparency and community collaboration to the greatest extent possible. The MOU development process took from May - September 2019. Key components of the MOU mandated that all ALPR data be secure and must have encryption requirements from the data source capture through transmission to the NCRIC data center for storage. The data would be stored in the NCRIC facilities in the Federal Building in San Francisco. NCRIC offices have 24/7 staffed security, multiple locked doors requiring both electronic keys and knowledge-based PINs. It also requires that only active NCRIC employees who possess a valid security clearance of SECRET or better are allowed physical access. Lastly NCRIC requires all activity is logged for audit and tracking purposes. Audits are available for an agency to view the actions of their officers.

The MOU specifically limits the retention of ALPR data collected from the BART ALPR cameras to 30-days, except where required by a subpoena, court order, or ongoing investigation. Additionally, the MOU specifically prohibits sharing of ALPR data collected from the BART owned cameras with federal immigration officials or immigration agencies either directly or indirectly. Authorized access to ALPR data in the NCRIC database is restricted to authorized public safety entities who possess a need to know and right to know the shared data except where explicitly denied by BART.

Computer Domains with NCRIC ALPR data access		
fremont.gov	unioncity.org	srpd.org
sanjoseca.gov	ncric.ca.gov	riversidesheriff.org
dalycity.org	placer.ca.gov	ci.el-cerrito.ca.us
ssf.net	wildlife.ca.gov	losbanos.org
sfgov.org	ACGOV.ORG	so.cccounty.us
sanleandro.org	countyofnapa.org	mendocinocounty.org
oaklandnet.com	sonoma-county.org	ci.berkeley.ca.us
fbi.gov	sunnyvale.ca.gov	danville.ca.gov
turlock.ca.us	santaclaraca.gov	pd.broadmoor.ca.us
doj.ca.gov	cityofconcord.org	ci.milpitas.ca.gov
cityofvallejo.net	cityofsanmateo.org	sebpd.com
smcgov.org	sanbruno.ca.gov	dmv.ca.gov
newark.org	hayward-ca.gov	belmont.gov
cityofberkeley.info	usdoj.gov	ociac.ca.gov
oaklandca.gov	nps.gov	burlingamepolice.org
chp.ca.gov	uspsoig.gov	yolo911.org
losaltosca.gov	state.gov	ci.healdsburg.ca.us
cityofpaloalto.org	ebparks.org	ic.fbi.gov
ci.irs.gov	colma.ca.gov	co.santa-cruz.ca.us
shf.sccgov.org	cityofvacaville.com	

Complaints

BART has not received any complaints with ALPR technology installed at Macarthur Parking Garage. BART regularly receives complaints from passengers who have been victimized by property crimes in the District's parking lots. ALPR technology is one of the tools that they District may use to deter criminal activity in the parking lots.

Surveillance Policy Compliance

There were no violations of the Surveillance Use Policy for the ALPR technology. A review of the NCRIC ALPR audit log revealed that the BART Police Crime Analyst has requested ALPR Data on twelve occasions from May 13-29, 2020. All twelve requests were for a specific police case number requesting information on stolen, wanted or suspect vehicles.

Crime Statistics

The ALPR cameras were installed in February 2020. Comparing the period of February through June for property crimes occurring in the Macarthur Parking Garage between 2019 and 2020, there were 9 incidents in 2019 and 7 incidents in 2020. There currently is insufficient data to establish a link between the deployment of ALPR technology and property crime rates at this location.

The COVID-19 pandemic also impacted ridership and parking in 2020, making a comparison between the time periods difficult. Additionally, the COVID-19 pandemic has impacted training and the BART Police Department has not yet had the opportunity to fully train employees on how to use the ALPR data generated by this project for investigative purposes.

BART crime statistics are updated monthly and made available at the following URL's;
https://www.bart.gov/about/police/reports
https://www.crimemapping.com/map/agency/454

Public Records Act Requests

BART has not received any public records requests for data collected by the ALPR system. One public records request was received in 2019 for information about which agencies BART shares ALPR data with.

Costs

The total cost for reinstalling the ALPR cameras at the Macarthur Parking Garage was $2,050.00. Beyond the installation costs for the Board approved project, ongoing maintenance will require 8-hours of labor every 180-days totaling approximately $1,200 per year. There is no cost for the services provided by the MOU with the NCRIC. BART is working on developing a future procurement for additional ALPR cameras to be used for both law enforcement and parking enforcement purposes.

6. BART Research Data Collection

2020 Surveillance Annual Report

Surveillance Technology Use

Description:

BART conducts research for a variety of research and learning purposes, such as to:

- Provide market information and metrics to help inform District decisions related to strategic planning, budget priorities, station access policy, marketing strategy, and other areas.
- Gather insight into latent demand, usage of TNCs and other emerging travel modes, and understand impact on public transit usage.
- Understand effectiveness of marketing initiatives by analyzing riders' aggregate travel behavior changes over time.
- Identify reasons for change in ridership patterns.

Methodologies using electronic and/or mobile data collection may be used to facilitate the following:

- Faster and less expensive data collection by eliminating the need to manually enter survey results.
- Expanded research capabilities using real time and location-based mobile technologies.
- "In the moment" ratings of BART facilities to improve rating accuracy, and image data that helps explain the reasons for ratings.
- The use of research panels to detect changes in travel patterns over time.
- Analysis of Bay Area residents' travel behavior, e.g., trip purposes, travel modes, travel mode shifts, vehicle occupancies, changes in car ownership habits, as well as demographics (for both riders and non-riders) in soliciting respondent consent for BART research projects.

BART discloses the types of data that will be collected, the nature of potential uses of such data by BART and, as applicable, third party partners in research, and describe the mitigations taken to protect respondent privacy.

Data Sharing

BART research data is not shared with any third party unless such disclosure is required by law or court order, or if shared under an agreement that ensures that the requirements of the Surveillance Use Policy (SUP), approved by the Board in 2018, are met. For example, BART may transfer select data to consulting firms or governmental organizations to use for travel modeling or environmental impact assessment, provided that data handling and security requirements are met. In such cases, where data at the individual record level are required for analysis, the third party will be required to be under contract with BART or bound by a Non-Disclosure Agreement (NDA) with BART. Such contracts and NDAs require adherence to provisions of this SUP and associated Surveillance Impact Report.

The District shared data with the following Authorized BART Service Providers for purposes of statistical analysis, transit modeling and transit system capacity analysis:

Authorized BART Service Providers	
The Behavioralist	The Steer Group

Complaints

There were no complaints received for the Data Collection and Usage for Research and Learning surveillance technology.

Surveillance Policy Compliance

There were no violations of the Surveillance Use Policy for the Data Collection and Usage for Research and Learning surveillance technology discovered during this period. No audit was conducted during this initial reporting period.

Crime Statistics

Not applicable. This solution is not a Crime Prevention tool.

Public Records Act Requests

There were no public records act requests for the Data Collection and Usage for Research and Learning surveillance technology.

Costs

The annual software license fee is approximately $30,000.

7. BART Trip Verification Technology

2020 Surveillance Annual Report

Surveillance Technology Use

Description: The Trip Verification Software (TVS) was developed to be used by BART staff and authorized service providers to provide the transit-riding public with new features and benefits. Handheld Trip Verification Devices (TVDs) were designed to be used to scan Clipper cards to grant access to unique BART or partner incentives aimed at increasing transit ridership. The initial deployment of the technology was to be used to incentivize travelers to take public transit to the San Francisco International Airport (SF0); however, the pilot implementation was postponed due to COVID-19. BART, SFO and the other stakeholders involved are waiting for favorable market conditions to move forward with the pilot. When the pilot is deployed, travelers who use Clipper to ride public transit to SFO will be entitled to use a priority lane (queue jump) through Airport security for ticketed airline passengers at designated terminals, saving time at the airport.

Data Sharing

This is a pilot program between BART, the San Francisco International Airport (SFO), San Francisco County Transportation Authority (SFCTA), and SAMTRANS. In compliance with the Surveillance Use Policy, limited data is made available to the agencies listed above on a mobile handheld device in order to confirm eligibility for qualifying incentives by scanning fare media. No other disclosures have been made.

Complaints

None received.

Surveillance Policy Compliance

There were no violations of the Surveillance Use Policy for the Trip Verification technology discovered during this period. No audit was conducted during this initial reporting period.

Crime Statistics

Not applicable. This solution is not a Crime Prevention tool.

Public Records Act Requests

There were no public records act requests for the Trip Verification technology.

Costs

Per the approved Surveillance Impact Report for Trip Verification Technology, the start-up development costs for the trip verification technology included the software development, hardware (android phones), device management and an initial marketing strategy for a total of $40,000**.**

Attachment B

Surveillance Use Policy
BART Automated License Plate Recognition (ALPR)

BART Police and Customer Access Departments
BPD-ALPR-SUP-02
21 Day BART Board Notice –October 3rd, 2019
15 Day Public Notice – October 9th, 2019
Board Meeting – October 24th, 2019

A. Purpose

The use of Automated License Plate Recognition (ALPR) technology seeks to increase the confidence of the public while using BART's public transportation system. Specifically, this technology seeks to improve the safety and protection of BART patrons, employees and their vehicles while in BART owned and operated parking areas and garages. In the future, BART may also consider use of ALPR for parking lot density and potential fee compliance. The ALPR system would record images of vehicle license plates in BART Parking locations. This technology is currently being used by a wide variety of agencies throughout the State of California for both Law Enforcement functions and parking functions. One of the most notably recognizable uses is by the FasTrak system, by the Bay Area Toll Authority for the purposes of fee collection over toll bridges, toll roads and high occupancy vehicle (HOV) express lanes. San Francisco International Airport (SFO) also uses ALPR technology at parking garages at SFO. The proposed implementation of the ALPR system in BART Parking areas would serve the following key purposes:

Crime Prevention

- Reduce the fear of crime and reassure the public and employees of being able to safely park their car in BART parking facilities, which will result in greater ridership for BART.
- Collect license plate numbers to assist in the identification, apprehension and prosecution of criminal offenders.
- Provide evidential support to prosecute offenders for criminal offenses.
- Provides both riders and employees a means of redress against property crimes, such as burglary and auto theft.

Efficient Parking Program Compliance

- Provides a uniform methodology for the enforcement of BART's parking rules.
- Aids in dispute mediation and provides documentation support for complaint resolution.
- Streamline parking validation.
- Help to increase ridership by determining parking lot density and space availability through and enhance efficient enforcement that parking is available only for BART passengers.
- Allow for the capability to automate parking fee collection in the future.

<u>Location of ALPR and Associated Cameras</u>

The ALPR come in three formats and include Fixed, Mobile or Hand-Held units. Fixed units may be installed in the following locations:

Fixed: Installed in BART owned and/or operated parking facilities, areas and structures.

Mobile: may be installed in the following locations:
On BART Law Enforcement Vehicles

Hand-Held: By Parking Enforcement Officers.

B. Authorized Use

License plate images captured by ALPR shall be used only to advance the BART purposes identified in this section and in Section A of this Policy. Use of the ALPR system and associated cameras will take place 24 hours a day, 7 days per week, and 365 days per year within all San Francisco Bay Area Rapid Transit District parking properties and parking properties owned and operated by BART. The ALPR system shall be used in in compliance with the District's Surveillance Ordinance and California Civil Code 1798.90.51 and 1798.90.53. The cameras shall not be used in areas where there is a reasonable expectation of privacy, such as off BART property, and shall not be used to harass, intimidate, or discriminate against any individual or group.

For purposes of this Use Policy, BART purposes include use for BART criminal investigations and to monitor activity to protect against harm to persons and property. It shall be permissible for data collected from the cameras to be used for the following public safety and BART investigation purposes:

- To assist in identifying and preventing crimes against persons and property;
- To locate missing children, adults, and/or elderly individuals, including in response to Amber Alerts and Silver Alerts;
- To assist in identifying, apprehending, and prosecuting criminal offenders;
- To assist in gathering evidence for administrative, civil, and criminal investigations and court actions in accordance with California State Law;
- To help Law Enforcement and Public Safety Personnel respond to emergency events;
- To assist in investigating and resolving staff and customer complaints and/or issues;
- To locate stolen, wanted, and/or other vehicles that are the subject of investigation;
- To locate and/or apprehend individuals subject to arrest warrants.
- To locate victims, witnesses, suspects, and others associated with a law enforcement investigation;
- To support local, state, federal, and regional Law Enforcement departments in the identification of vehicles and drivers associated with criminal investigations, including investigations of serial crimes;
- To protect participants at special events;
- To protect BART Parking Facilities.
- Parking efficiency and enforcement

Administrative functions of ALPR data used for criminal enforcement purposes will be managed by BART and the Northern California Regional Intelligence Center (NCRIC). Any data obtained from ALPR technology shall be used and handled pursuant to this use policy, BART's Surveillance Use Ordinance and applicable State and Federal law.

BART Police shall be permitted to review ALPR Data Images to protect and to respond to law enforcement inquiries, to investigate complaints by customers and employees, and to provide law enforcement authorities with ALPR Data when legally required to do so. All other uses not referenced in this document shall be prohibited. ALPR technology shall not be used for personal or non-law enforcement or parking efficiency purposes and shall adhere to the Surveillance Ordinance.

C. Data Collection

Data collection shall be limited to vehicles entering, exiting and parking on BART owned and operated property. Collection may include information on the vehicle license plate and the image of the vehicle. Routine Data Collection shall not be stored beyond 30 days, except when lawfully required to by subpoena, court order or during an ongoing investigation. Data used to substantiate parking citations will be retained for 5 years to allow time for citation appeal and identification of scofflaws.

D. Data Access

Access to ALPR Data shall be restricted to the following personnel:

- All persons designated by the BART Police Department.
- Designated NCRIC Staff involved in the ALPR Administration.
- BART personnel involved in the operation, installation and maintenance of the ALPR system.
- Customer/Public Access (Restricted per the Surveillance Ordinance in item G)
- Per Court Order or Subpoena, or during an ongoing investigation.
- Office of Independent Police Auditor and Internal Affairs Department
- District Legal Affairs Department
- Authorized BART Service Providers hosting parking efficiency and enforcement applications

E. Data Protection

The data collected by the ALPR system that is used for criminal enforcement purposes will be maintained in a secure manner between the BART Police Department and the NCRIC where physical access is limited to authorized individuals and includes physical access protections and firewalls.

Data used for parking efficiency and enforcement purposes will be separately stored and maintained in a secure location where physical access is limited to authorized individuals and includes physical access protections and/or firewall protections from external intrusion.

All ALPR data shall be maintained in a secure manner and be encrypted via BART's IT encryption requirements from the data source capture through transmission and storage.

Data used for criminal enforcement purposes that is stored in the NCRIC offices in the federal building in San Francisco shall maintain 24/7 staffed security, multiple locked doors requiring both electronic keys and knowledge-based PINs and limit access to active NCRIC employees that also possess a valid security clearance of SECRET or better.

- All activity is logged for audit and tracking purposes. Audits are available for an agency to view the actions of their officers.

F. Data Retention

Staff will adhere to the District's Surveillance Ordinance. All data from the ALPR be collected, retained and stored in accordance with BART Surveillance Ordinance. Data captured from the ALPR and camera system will automatically be downloaded onto a secure data storage system where it will be stored based on the systems' design and recording capabilities before being overwritten by new data; which is thirty (30) days as outlined in section 707.1.5 of BART Surveillance Ordinance. Data shall not be stored beyond 30 days except when lawfully required to by subpoena, court order or during an ongoing investigation. Further a written Memorandum of Agreement with the NCRIC shall specify the retention policy of the ALPR data is only retained for the period as specified by the originating agency (BART). The creation date is automatically tracked for every ALPR data point, and once the lifespan of that point is exceeded, it is removed via automated nightly processes.

Data used to substantiate parking citations will be retained for 5 years to allow time for citation appeal and identification of scofflaws (vehicles with multiple unpaid citations).

G. Public Access

BART shall grant Public access to data collected from the ALPR system per BART Surveillance Ordinance 707.1.8, 707.1.9 only in accordance to California State Law. Information gathered will not be disclosed to the public unless such disclosure is required by law or court order. The BART Police Department is subject to BART's Surveillance Ordinance that has been publicly noticed and approved by the BART Board. ALPR Data Collection will be monitored by BART Police as well as be subject to Police Internal Affairs and State Auditors to ensure the security of information and compliance with applicable privacy laws.

Such data will not otherwise be disclosed/released by the BART Police Department without the consent of the Chief of Police and District Legal. If an ALPR operator is required to provide access to ALPR information, the ALPR operator shall do the following:

(a) Maintain a record of that access. At a minimum, the record shall include the following:
(1) The date and time the information is accessed.
(2) The license plate number or other data elements used to query the ALPR system.

(3) The username of the person who accesses the information, and, as applicable, the organization or entity with whom the person is affiliated.
(4) The purpose for accessing the information.
(b) Require that ALPR information only be used for the authorized purposes described in the usage and privacy policy.
(1) Indicate the authorized use; such as for criminal investigation.

707.1.8 RELEASE OF ALPR DATA TO THE GENERAL PUBLIC

All ALPR Data shall be used by law enforcement for public safety, security, and parking efficiency/enforcement purposes only; except as required by law, subpoenas or other court process, such data will not otherwise be disclosed/released by the BART Police Department without the consent of the Chief of Police and District Legal.

Department employees shall not release any information, including capabilities regarding the District's ALPR systems to the public without prior authorization from the Chief of Police, or District Legal.

707.1.9 REQUESTS FOR VIDEO IMAGES FROM THE MEMBERS OF THE PUBLIC

Persons that have a subpoena or preservation letter, and are interested in requesting ALPR, shall be directed to the Department's Records Division during normal business hours, or via fax at 510- 464-7089 for consideration of their request. Records shall consult with the Chief of Police and District Legal Prior to any approval of release.

Persons that do not have a subpoena or preservation letter and are interested in requesting ALPR Data are to be directed to the District Secretary's Office for review by District Legal at 510-464-6080 or via fax at 510-464-6011.

H. Third Party Data Sharing

BART shall maintain robust security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure. The Administrator of the data collection will not share information with ICE or any agency conducting immigration enforcement or removal operations. Information is only shared with other law enforcement possessing a need and legal right to know, including the following:

- In response to subpoenas
- Pursuant to a Court Order
- Request by Law Enforcement Agencies for active Criminal Investigations
- In accordance with all applicable California State law

BART will retain all ownership rights to the data. Private vendors cannot share the data unless directed to by BART in writing and in accordance with this policy, and will forward any subpoena requests for the data to BART.

Notwithstanding any other law or regulation:
(a) A public agency such as BART that operates or intends to operate an ALPR system shall provide an opportunity for public comment at a regularly scheduled public meeting of the governing body of the public agency before implementing the program. BART shall present this Impact and Use document to the BART Board of Directors and provide notice to the public in accordance with BART's Surveillance Ordinance. BART Police Department shall also conduct outreach with privacy groups to address any privacy concerns that may be raised.

(b) A public agency shall not sell, share, or transfer ALPR information, except to another public agency, and only as otherwise permitted by law. For purposes of this section, the provision of data hosting or towing services shall not be considered the sale, sharing, or transferring of ALPR information.

I. Training

Training for BART's ALPR system will be provided by BART internal staff and by ALPR service providers and the NCRIC. Training will consist of ALPR operation, installation, data protection and administration of the ALPR System and ALPR Data. Technical training will be both hands on and via electronic instruction.

J. Auditing and Oversight

The BART Police Department shall oversee the BART ALPR System and data retention to ensure compliance with the Surveillance Ordinance. Additionally, both BART Police will require the management of the system to be open for administrative auditors to ensure the Surveillance Ordinance and California State Laws are adhered. The audit process shall ensure that no misuse of the system or parts of the system occurs. Additionally, a secondary check with the reporting agency will be required by BART Police to adjudicate all crimes prior to taking enforcement action on crimes that are not a crime in progress or otherwise present exigent circumstances.

Personnel who are authorized to have access to the system shall be designated in writing and the designation shall ensure that their access to and use of the data complies with the Ordinance.

A log shall be maintained that records when access to ALPR data is requested. This shall include the date, time, data record accessed, and staff member involved. The log shall be available for presentation for all required audits.

Surveillance Impact Report
BART Automated License Plate Recognition (ALPR)

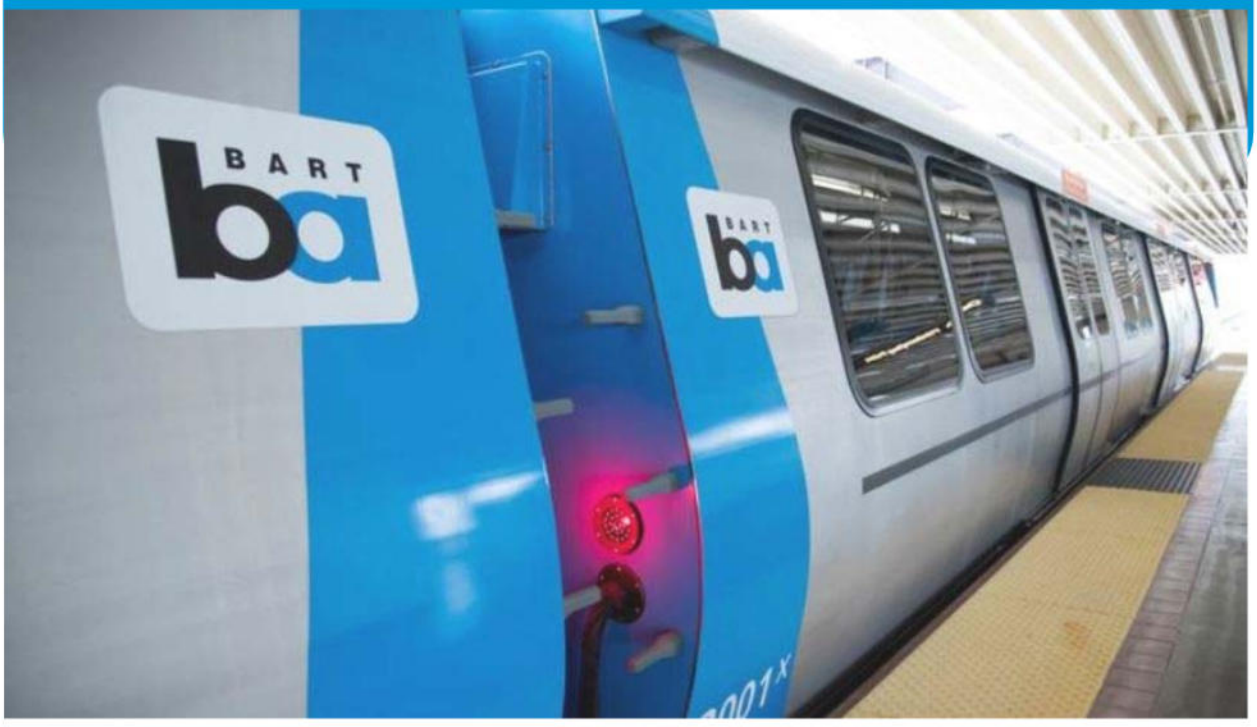
BART Police and Customer Access Departments

BPD-ALPR-SUP-02

21 Day BART Board Notice – October 3rd, 2019

15 Day Public Notice – October 9th, 2019

Board Meeting – October 24th, 2019



A. Information describing the proposed surveillance technology and how it generally works.

Automated License Plate Recognition (ALPR) systems are camera technologies that can capture vehicle license plate images and a portion of the vehicle. This technology will be used for the safety and security of patrons and employees and protection of their vehicles while using BART owned and operated parking facilities.

ALPR systems may include Fixed visible, mounted technologies. Mobile scan options include mobile units which can be mounted to a police car. Future use may include hand held options and mobile units may be considered parking program enforcement by roving parking enforcement officers.

ALPR technology increases law enforcement's ability to recover lost/stolen property and provide evidentiary support for criminal prosecution. In 2012 the RAND Corporation conducted a study on ALPR Technologies across the United States and found that ALPR was responsible for increasing Stolen Vehicle recovery by 50%. (RAND, Safety and Justice Program; *ALPR for Law Enforcement Opportunities and Obstacles*).

Currently, the ability for BART police to solve crimes such as auto burglaries and thefts is greatly reduced due to a lack of video evidence. ALPR technologies records images of a vehicle's license plate. The image, when compared against a hot list provides information that the vehicle may have been used in a crime. This information often leads to a timelier ability to capture offenders. Accurate information provided to BART Police will increase the ability to successfully prosecute offenders and greatly increase the chances of returning stolen property to the victim.

B. Information on the proposed purpose(s) for the surveillance technology.

Implementation of the proposed BART ALPR technology system would serve the following key purposes:

- Aid in the recovery of lost or stolen vehicles.
- Prevent, deter and detect crime, damage to patron and employee vehicles.
- Reduce crime and in doing so, reassure the public and employees using BART owned and operated Parking Facilities.
- Assist in the monitoring, identification, apprehension and prosecution for criminal offenses.
- Aid in the Investigation of complaints or offenses and provide evidentiary support upon which to take criminal and civil penalty actions.
- Parking efficiency and enforcement

C. Recommendation for Fixed Reader Installations location(s), to be deployed, based on current statistics for Auto Theft and Auto Burglary.

- A10 – Lake Merritt 5/2 Low Priority Installation
- A20 – Fruitvale 26/16 Priority Installation
- A30 – Coliseum 21/23 Priority Installation
- A40 - San Leandro 21/17 Priority Installation
- A50 - Bay Fair 24/9 Priority Installation
- A60 – Hayward 21/21 Priority Installation
- A70 – South Hayward 17/16 Priority Installation
- A80 – Union City 10/3 Low Priority Installation
- A90 – Fremont 9/5 Low Priority Installation
- L10 - Castro Valley 1/9 Low Priority Installation
- L20 - West Dublin 5/3 Low Priority Installation
- L30 - Dublin / Pleasanton 18/8 Priority Installation
- K10 – 12th Street 0/0 N/A
- K20 – 19th Street 8/4 Low Priority Installation
- K30 – MacArthur 3/2 Low Priority Installation
- R10 – Ashby 4/5 Low Priority Installation
- R20 – Berkeley 0/0 N/A
- R30 – North Berkeley 4/11 Priority Installation
- R40 – El Cerrito Plaza 4/5 Low Priority Installation
- R50 – El Cerrito Del Norte 15/14 Priority Installation
- R60 – Richmond 9/22 Priority Installation
- C10 – Rockridge 6/4 Low Priority Installation
- C20 – Orinda 5/7 Low Priority Installation
- C30 – Lafayette 4/2 Low Priority Installation
- C40 – Walnut Creek 1/4 Low Priority Installation
- C50 – Pleasant Hill 5/4 Low Priority Installation
- C60 – Concord 16/10 Priority Installation
- C70 – North Concord 18/14 Priority Installation
- C80 – Pittsburg Pay Point 27/13 Priority Installation
- M10 – West Oakland 20/9 Priority Installation
- M16 – Embarcadero 0/0 N/A
- M 30 – Powell 0/0 N/A
- M 20 – Montgomery 0/0 N/A
- M 40 – Civic Center 0/0 N/A
- M 50 – 16th Street 0/0 N/A
- M60 – 24th Street 0/0 N/A
- M70 – Glen Park 0/0 N/A
- M80 – Balboa Park 0/0 N/A
- M 90 – Daly City 13/13 Priority Installation

- W10 – Colma 1/3 Low Priority Installation
- W20 – South SF 1/0 Low Priority Installation
- W30 – San Bruno 0/1 Low Priority Installation
- W40 – Millbrae 2/1 Low Priority Installation
- Y10 – SFO 0/0 N/A
- S10 – Irvington (Future) 0/0 TBD
- S 20 – Warm Springs 1/7 Low Priority Installation
- S 40 – Milpitas 0/0 TBD
- S 50 – Berryessa 0/0 TBD
- E 20 – Pittsburg Center 0/0 Low Priority Installation by Operating Contractor
- E 30 – Antioch 0/12 Priority Installation by Operating Contractor
- Hercules Park-and-Ride
- Isabel (Livermore) Park-and-Ride
- Laughlin (Livermore) (Park-and-Ride)
- Irvington (Fremont) (future station)
- All future BART station parking facilities, either owned, operated and/or managed by BART and intended for BART passengers.

A. Crime statistics used to determine location installation, to deter or detect crime.

Statistics on Auto Burglary Auto Theft and Catalytic Converter Theft were used to provide recommended priority installations. The proposed implementation of the ALPR System is part of an overall Districtwide security system with functions for crime deterrence and detection, as well as future considerations for a more efficient parking program enforcement through automation. The proposed ALPR system would target hot spots crime areas as identified by the Crime Analysis Unit. Additionally, statistics were used to outline the problem expressed by BART Riders. Numbers for Auto Burglary, Auto Theft and Catalytic Converter Theft were analyzed for 2018 through March of 2019. The cost benefit analysis below was used in part to determine the viability of this technology.

Current Annual Crime Statistics	**2018**	**2019 (March)**	**15 Month Average**
Auto Burglary:	198	264	231
Auto Theft:	102	43	145
Catalytic Converter Theft:	205	51	128

Cost Benefit Analysis		**Cost to BART Riders**
Auto Burglary: (Average Deductible and Property)	$1,000 x 231 cases annually =	$231,000
Auto Theft: (No comprehensive Insurance)	$15,000 x 145 cases annually =	$2,175,000
Catalytic Converter Theft: (Average cost w/labor)	$1,500 X 128 cases annually =	$192,000
	Total Loss for 15 Months	**$2,598,000**

Approximate cost of a fixed ALP Reader is between $15,000 to $22,000 per installed unit, for 16 Priority Installations total cost $352,000 for one ALPR at all recommended parking areas.

B. An assessment identifying any potential impact on privacy rights and discussing any plans to safeguard the rights of the public.

Data collection by the ALPR System includes information found on the vehicle license plate. BART recognizes that all people have an inalienable right to privacy and BART is committed to protecting and safeguarding this right.

In 2013, data experts introduced to the public the concept of "meta data", which detailed that larger data can be gathered from individual data points. A recent example included, that by using a simple homemade app that captured simple data points such as phone number called, and time of day, Stanford lawyer and computer scientist Jonathan Mayer was able to accurately identify 80% of the volunteers in his study, using only open source databases such as Yelp, Facebook, and Google. Among the many individuals he identified, he successfully identified a woman that had an abortion, another woman that had cancer, and a man collecting guns and growing marijuana in his home.

Today, data scientists can accurately identify over 95% of individuals based solely on 4 geospatial (time, location) "meta data" points. Human are creatures of habit, typically driving the same way to work, our house of worship, and our neighborhood grocery store. Current attempts to "de-identify" or anonymize data are insufficient, due to modern day computing power and the sheer collection of data points available from public and private sources. License plate scans are collected by both public and private parties, and often shared via large commingled databases accessible by a simple subscription service.

In recognition of these concerns, BART has taken the following steps to mitigate the potential risk inherent in collecting this data from its customers.

As discussed in this Report and the Surveillance Use Policy, only authorized BART personnel, authorized NCRIC personnel or outside law enforcement pursuant to a court order or subpoena, will have access to this data for the purposes identified in this report and in the Surveillance Use Policy. BART and NCRIC shall maintain robust security procedures and practices, including multi layered engineering and administrative protections with the following details: CARD access locked doors with restricted and approved access only for designated personnel. Restricted Administrative rights to data access to provide operational, administrative, technical, and physical safeguards, to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure. BART and NCRIC shall not provide data to federal immigration agencies. Data shall not be stored beyond 30 days, unless lawfully required by subpoena, court order or during an ongoing investigation.

C. The fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding.

Initial Purchase Cost
Based on an estimated budget, the cost is approximately $15,000 to $22,000 per installed ALPR unit. Costs for ALPR mobile units for enforcement vehicles would be approximately $20,000 per vehicle.

Personnel Costs
BART personnel could provide installation for the ALPR System, which is estimated to be approximately $100,000 at normal BART labor rates. However, depending upon the complexity of the installation and the availability of BART labor, the ALPR vendor may also provide ALPR installation at significant cost savings to BART when negotiated into the ALPR purchase contract.

Ongoing Costs
The ongoing costs associated with the deployment of a systemwide ALPR System will be primarily preventative and corrective maintenance costs. There may also be an annual leasing software for the ALPR units used for parking enforcement, depending upon contract details, which is estimated initially to be about $200,000 annually.

The anticipated lifespan of the ALPR system is about ten (10) years. However, with proper maintenance staff, anticipates the useful operational lifespan of the system could be extended.

Potential Sources of Funding
- FTA Security Grant
- Operating Funds
- FEMA Grants
- Bonds
- Parking Fee Revenue

D. Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis.
Yes, third party in the way of vendor support may require the use of log files and sample image data to be collected for analysis of errors and system malfunctions. The data is not stored after any maintenance or trouble shooting is complete.

The Northern California Regional Intelligence Center (NCRIC) will be the handling center for the captured data that will be accessed by BART Police for law enforcement investigative purposes.

Data used for parking enforcement purposes may be shared with authorized BART Service Providers hosting parking efficiency and enforcement applications.

E. A summary of alternative methods (whether involving the use of a new technology or not) considered before deciding to use the proposed surveillance technology, including the costs and benefits associated with each alternative and an explanation of the reasons why each alternative is inadequate or undesirable.

BART examined the current capabilities for preventing and deterring auto burglary and auto. The current law enforcement system uses manpower to physically verify a crime in progress and conduct investigations. The current system is both labor intensive and not highly effective for preventing or deterring auto crimes. As parking lots continue to expand beyond the 47,000 parking spaces, enforcement actions are not able to keep pace with the criminal activity in these new locations. Currently the enforcement actions are limited to observing a crime in progress and catching criminal activity in the parking areas. Statistics from Federal and State Criminal Apprehensions indicate that more than 70% of crimes are committed by people using vehicles. There is currently no method for vehicles entering BART parking areas to be identified. Without this technology, identification of vehicles and associated criminals' activity is limited to observing crime in progress or limited investigative recovery. There is no alternative technology that can meet the needs of the District. The benefits and disadvantages of ALPR are:

Benefits of ALPR

- Improves public safety and security.
- Gives BART Riders using BART Parking Facilities a redress for crimes against their persons and property.
- Provides documentary evidence for prosecution.
- Enhances public confidence when Parking at BART.
- Offers low maintenance operating costs.
- Requires minimal training of personnel on the use of the technology.

Disadvantages of ALPR

- Requires initial installation investment, although recoverable within a few years' time.
- Must be protected from vandalism.
- Privacy risk to customers that use BART Parking Facilities from the collection of their locational data.

F. A summary of the experience, if any is known, other law enforcement entities have had with the proposed technology, including information about the effectiveness, any known adverse information about the technology such as unanticipated costs, failures, civil rights or civil liberties issues.

Many other Agencies, including a robust number of Law Enforcement Agencies use ALPR Systems throughout California and the Nation. ALPR System Efficiencies are 98% with a correct Read Rate of 95% resulting in high validity of documentation of incidents. Highly effective read rates protect individuals and civil liberties by ensuring proper, correct capturing of information.

BART would require Annual Certification of the System conducted by third party calibration service parties will ensure the system is maintained at factory read rates.

- California Highway Patrol and multiple County and City LE Agencies use ALPR Technologies for law enforcement function.
- SFMTA Uses ALPR Technologies.
- California State Universities including UC Berkley, Hayward and Merced use ALPR Technologies.
- CALTRANS uses ALPR Technologies for all Bridges, and Tolls via FasTrak which has been widely well received by the Public, with specific positive comments for FasTrak Fare collection and ease of use.
- San Francisco International Airport uses ALPR Technologies using FasTrak to pay for parking at airport lots.

Adverse information on ALPR Technology includes:

- ALPR can be fooled using false plates. Although if reported, this would show as a stolen plate in the ALPR System.
- ALPR System Data must be maintained, failure to do so could reflect old records in the system. It is imperative the agency (BART Police Department) implement a secondary verification procedure for all non-exigent or crimes in progress.
- Some individuals and privacy groups do not like the use of ALPR by law enforcement, because they feel it is an infringement of their privacy. ALPR Technologies record all license plates; including those that have not committed offences or infractions in addition to those that have.
- ALPR has a 95 percent correct read rate which means it also has a 5 percent incorrect read rate. This can be best managed by ensuring a robust policy on acceptable ALPR reads and secondary verification for non-crimes in progress.
- Inaccurate data in the system or inaccurate scans can lead to civil rights abuses. In 2015, the taxpayers of San Francisco paid $495,000 to Denise Green, a 45-year-old Muni driver after police officers pulled her over at gunpoint based on an erroneous alert from their system – the scan was off by one digit, and officers failed to verify its accuracy.

It is important to note that when used properly and judicially along with proper oversight and with written policies in place, ALPR can greatly enhance the safety and security of all personnel using BART owned and operated parking facilities. The State of California has the largest concentration of Agencies using ALPR, followed by New York and Florida. Enclosed below is a direct link to other California Agencies ALPR Use Policies.

- **Central Marin Police Authority**
- **City and County of San Francisco**
- **City of Alameda**
- **City of Alhambra**
- **City of American Canyon**
- **City of Anaheim**
- **City of Antioch**
- **City of Arcadia**
- **City of Arcata**
- **City of Atherton**
- **City of Auburn**
- **City of Avenal**
- **City of Azusa**
- **City of Bakersfield**
- **City of Beaumont**
- **City of Bell**
- **City of Bell Gardens**
- **City of Berkeley**
- **City of Belvedere**
- **City of Beverly Hills**
- **City of Brawley**
- **City of Brea**
- **City of Brentwood**
- **City of Brisbane**
- **City of Buena Park**
- **City of Burbank**
- **City of Burlingame**
- **City of Campbell**
- **City of Carlsbad**
- **City of Chico**
- **City of Chino**
- **City of Chula Vista**
- **City of Claremont**
- **City of Clayton**
- **City of Clovis**
- **City of Concord**
- **City of Corning**
- **City of Corona**
- **City of Coronado**
- **City of Covina**
- **City of Culver City**
- **City of Cypress**

- **City of Daly City**
- **City of Davis**
- **City of Dublin**
- **City of El Cajon**
- **City of El Centro**
- **City of Elk Grove**
- **City of Emeryville**
- **City of Escondido**
- **City of Fairfield**
- **City of Folsom**
- **City of Fontana**
- **City of Fountain Valley**
- **City of Fremont**
- **City of Fresno**
- **City of Fullerton**
- **City of Galt**
- **City of Gardena**
- **City of Glendale**
- **City of Glendora**
- **City of Hanford**
- **City of Hawthorne**
- **City of Hayward**
- **City of Huntington Beach**
- **City of Imperial**
- **City of Inglewood**
- **City of Irvine**
- **City of Irwindale**
- **City of La Habra**
- **City of La Mesa**
- **City of La Palma**
- **City of La Verne**
- **City of Laguna Beach**
- **City of Lemoore**
- **City of Livermore**
- **City of Lodi**
- **City of Long Beach**
- **City of Los Alamitos**
- **City of Los Altos**
- **City of Los Gatos**
- **City of Madera**
- **City of Manhattan Beach**
- **City of Manteca**
- **City of Menlo Park**

- **City of Milpitas**
- **City of Modesto**
- **City of Monrovia**
- **City of Monte Sereno**
- **City of Morgan Hill**
- **City of Montclair**
- **City of Montebello**
- **City of Monterey Park**
- **City of Moraga**
- **City of Mountain View**
- **City of Murrieta**
- **City of National City**
- **City of Newark**
- **City of Newport Beach**
- **City of Novato**
- **City of Oakland**
- **City of Oceanside**
- **City of Oxnard**
- **City of Pacifica**
- **City of Palo Alto**
- **City of Palos Verdes Estates**
- **City of Pasadena**
- **City of Petaluma**
- **City of Piedmont**
- **City of Pismo Beach**
- **City of Pittsburgh**
- **City of Placentia**
- **City of Placerville**
- **City of Pleasant Hill**
- **City of Red Bluff**
- **City of Redlands**
- **City of Redwood City**
- **City of Richmond**
- **City of Ripon**
- **City of Riverside**
- **City of Sacramento**
- **City of San Bernardino**
- **City of San Bruno**
- **City of San Diego**
- **City of San Fernando**
- **City of San Gabriel**
- **City of San Jose**
- **City of San Leandro**

- **City of San Luis Obispo**
- **City of San Marino**
- **City of San Mateo**
- **City of San Pablo**
- **City of San Rafael**
- **City of San Ramon**
- **City of Santa Clara**
- **City of Santa Monica**
- **City of Sausalito**
- **City of Seal Beach**
- **City of Sierra Madre**
- **City of Signal Hill**
- **City of Simi Valley**
- **City of South Beach**
- **City of South Gate**
- **City of South San Francisco**
- **City of Suisun City**
- **City of Sunnyvale**
- **City of Torrance**
- **City of Tulare**
- **City of Tustin**
- **City of Ukiah**
- **City of Upland**
- **City of Vallejo**
- **City of Vernon**
- **City of Visalia**
- **City of Walnut**
- **City of Walnut Creek**
- **City of West Covina**
- **City of West Sacramento**
- **City of Westminster**
- **City of Westmoreland**
- **City of Whittier**
- **City of Woodland**
- **County of Alameda**
- **County of Contra Costa**
- **County of Fresno**
- **County of Los Angeles**
- **County of Marin**
- **County of Orange**
- **County of Riverside**
- **County of Sacramento** (Sheriff)
- **County of Sacramento** (Department of Human Assistance)

- **County of San Bernadino**
- **County of San Diego**
- **County of San Luis Obispo**
- **County of San Mateo**
- **County of Santa Clara**
- **County of Shasta**
- **County of Solano**
- **County of Ventura**
- **County of Yolo**
- **California State University, Long Beach**
- **Kensington Police Protection and Community Services District**
- **Port of San Diego**
- **Town of Hillsborough**
- **Town of Los Gatos**
- **Town of Portola Valley**
- **Town of Tiburon**
- **University of California - Merced**

In conclusion, ALPR Technologies can offer greater safety and security for BART patrons and employees using BART Parking Facilities. Patrons will have an improved safety and security when parking at BART.

Inspector General/Independent Police Auditor Q&A/outline

Brian – intro guests

Sergio –Generally describe the role of an Inspector General – what are your primary duties? How (legal formation) and why (e.g. scandal, lawsuits, proactive) was your office created? Does your mission include individual disciplinary actions, or generally limited to pattern and practice/systemic matters?

Mark – You were provided with a great opportunity, the chance to build something from the ground up. Share with us the history of BART's inspector general office, and what it was like trying to get buy-in and resources to support your vision.

Russell– Before we get into more substantive topics, and having stepped into the literal same job that Mark had, do you believe that BART is honoring that original vision, maybe improved upon it, or backtracked?

Russell – In the 'before times' about two years ago, we had lunch and you were sharing with me a story about BWC recording buffers, and getting the POA to buy-in to a lengthier recording period of time. A lot of my questions for all three of you have a nexus to trust because it's the glue that holds our respective oversight functions together. Do you feel you have the trust of the POA, and how have you tried to increase trust amongst the various stakeholders so that you can do your job?

Sergio – Your predecessor was accused of being too cozy with the Sheriff. Expanding upon what Russell just described, how do you navigate being a watch dog, remain independent, and yet still get people with likely competing priorities and natural tensions, whether legal or turf, to trust you sufficiently to provide meaningful information to the Board and public?

Mark – As you know, I work on crafting surveillance technology oversight models across the country. I also Chair the City of Oakland's privacy commission, which serves as an advisory body within the tech vetting framework. We've recently discovered that we were being misled about certain audits being performed. I've had many administrative and legislative staffers contact me from other jurisdictions that operate in a similar framework as Oakland, and they all ask me if we have any proof that the required audits are being performed, because in their they're also not seeing any evidence of audits or are never provided any data to independently verify. The entire model's success hinges on trust in the representations from staff that are being provided to us in our oversight role. First, with your lawyer hat on – can you think of any alternate route for a non-sworn, volunteer commission to get access to raw data in order to indepently verify the claims being made, and if yes, should a layperson be given such access? Assuming the answer is No to either, my follow up question loops back to your first – how would a privacy commission like Oakland's go about advocating for its own IG – please be as specific as you care to be (budget, criteria for IG, meet and confer negotiations with POAs).

Sergio – Does the Orange County public know you exist? Do they take advantage of the complaint intake system? Has that led to any pattern and practice or system abuses that

warranted your office getting involved that you can share? Is it too early to guage whether the OC public is beginning to trust your office, after the past issues?

Russell – BART seems to have a knack for showing up on video when its misconduct is at its worse. Often, the videos go viral and the public typically instally rushes to judgment. I'm thinking of the Michael Smith and Andrea Appleton video, where Michael was slammed to the ground by BART PD, and Andrea was pinned down, while pregnant. She claims to have had a miscarriage as a result of this incident. The couple was represented by my former attorney Glenn Katon. In the same context as a tainted jury pool, does the public narrative interfere with your investigative efforts, or is it mostly a non-issue for someone that generally works behind the scenes before releasing a report? I would imagine when the electeds, the POA, and the general public are all breathing down your neck, it's not pleasant. What is the best result that can come about after your review and possible presentation to the CPRB or the Board of Directors? No matter what conclusion you reach, it seems like someone is going to be mad at you.

Sergio – As a state deputy attorney general, you worked on the Stephon Clark matter. In no small part because of that case, AB 392 was signed into law, which raised the standard for when use of force by police may be used. It's still in its infancy, but do we know enough at this time as to whether 392 is making a meaningful impact? I'm thinking of the watered down amendments that were made to keep the bill alive, like removing the term "necessary" and use of other qualifiers to limit the law's applicability. Do you see the need for more legislative authority (or amendments to improve existing law) that you can identify at this time?

Mark – Let's go back in time and talk about the Christopher Commission. We don't need a lengthy historical report, but if you would please summarize the what and the why, and how it's impacted your role and office today. Do you have objective data today that demonstrates any significant reduction in legal liability and misconduct payouts, or at least that LA is trending in the right direction? And on that note – how would you define success in the context of your particular job?

Sergio – We'll start with you, and I'd like Mark to weigh in as well as you've both dealt with Sheriffs. If you have also Russell, please jump in. Do you run into interference with any Sheriffs as to their alleged constitutional authority/autonomy when it comes to oversight, any claim that in their state agent capacity, neither you nor the Board have authority to look too deeply into their affairs? I have weekly nightmares about Gov Code 25303, the most ambiguous California statute I've seen. The CA Attorney Generals of the past don't seem to have much oversight of Sheriffs or aren't willing to act, and if the Board can't legally do much, how do we get a handle on what's happening in our Sheriff departments and jails? Will the McCarty oversight committee bill make much of an impact? Does subpoena power make a difference in practice?

Mark – Same questions.

Russell – If you were given a blank check by your Board, what would you do to improve your office?

Brian – closing remarks and thank guests.

How does the Surveillance Ordinance work in practice? Process for city to acquire or use a surveillance technology

Notification

- Police Dept. **notifies** Police Commission of its wish to acquire new surveillance technology.

Report Submission

- Police Dept. submits a **Surveillance Impact Report** and proposed **Surveillance Use Policy** to the Police Commission for its review at a regularly noticed meeting.

Commission Evaluation

- Police Commission reviews documentation, works with Police Department to revise Impact Report and Use Policy
- Recommends that the City Council **adopt**, **modify**, or **reject** the proposed Surveillance Use Policy.

Public Notice

- City Council provides **public notice** that will include the Surveillance Impact Report, proposed Surveillance Use Policy, and Police Commission recommendation at least fifteen (15) days prior to the public hearing.

Public Hearing

- City Council determination: 1) benefits to the community outweighs the costs; 2) proposal will safeguard civil liberties and civil rights; and 3) no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective.

Elements of the Required Documents

(Heart of the ordinance)

Surveillance Impact Report:

A. Description of the technology
B. Proposed use(s)
C. Location to be deployed
D. Impact on civil rights and liberties
E. Mitigations
F. Data types and sources
G. Data security
H. Fiscal cost(s)
I. Third-party dependence
J. Alternative methods
K. Track record

Surveillance Use Policy:

A. Purpose of the use
B. Authorized use(s)
C. Data collection
D. Data access
E. Data protection
F. Data retention
G. Public access
H. Third party data sharing
I. Training
J. Auditing and Oversight
K. Maintenance

Ongoing Oversight With Annual Reporting

Elements of the Report:

A. Description of How the Technology Was Used
B. Whether and How Often Data Was Shared With Outside Entities
C. A Breakdown of Where the Technology Was Installed or Used
D. A Summary of any Complaints Received
E. An Analysis of Whether the Use Policy Adequately Protected Civil Liberties
F. The Results of Any Internal Audits
G. Information About Any Data Breaches, and Responses thereto
H. Crime Statistics That Help The Community Assess Efficacy
I. Total Costs, Both Upfront and Ongoing

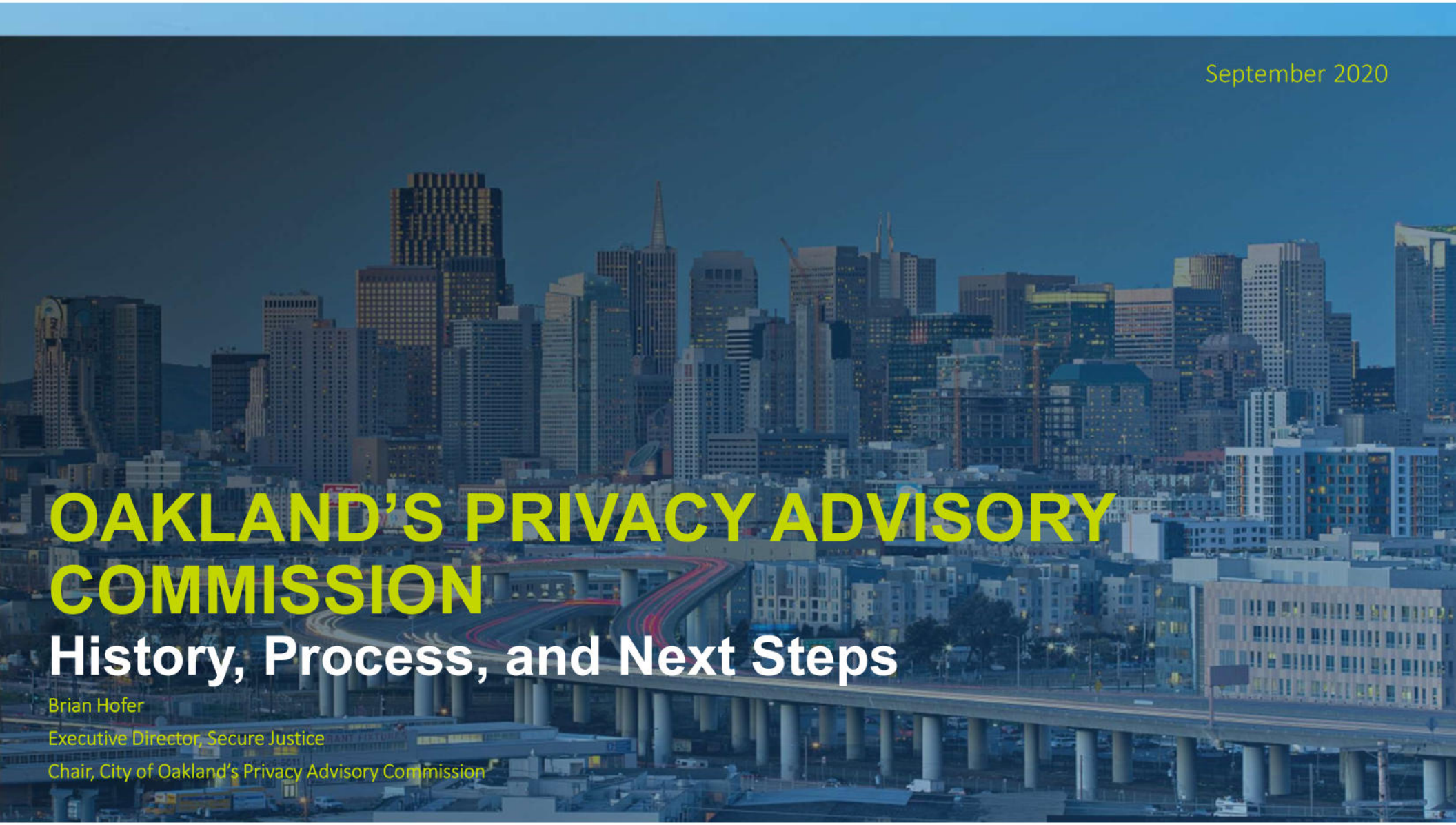
Questions?
Interested in engaging?

Please reach out!
We'd love to
hear from you.

brian@secure-justice.org

@b_haddy

@SecureJustice



September 2020

OAKLAND'S PRIVACY ADVISORY COMMISSION

History, Process, and Next Steps

Brian Hofer

Executive Director, Secure Justice

Chair, City of Oakland's Privacy Advisory Commission

The Opportunity

Oakland contemplated building-out a multi-faceted surveillance apparatus

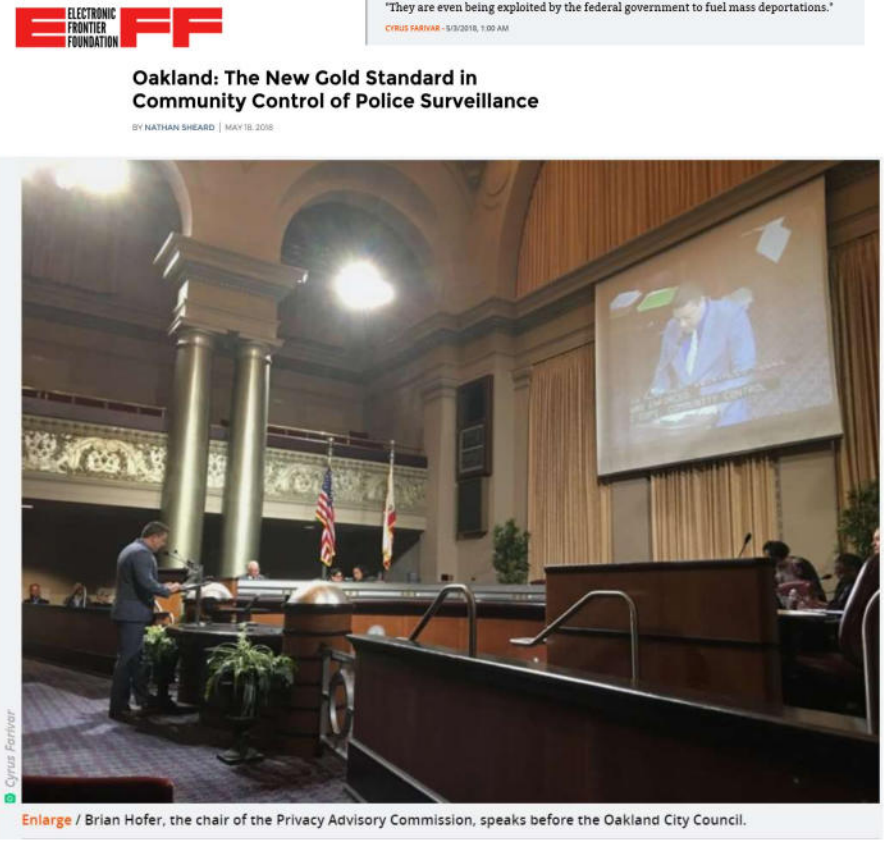
- In 2013, Oakland was given the opportunity to expand its Port's Domain Awareness Center
  - DHS would foot the $10.9M bill to build out a city-wide surveillance apparatus to fight terrorism and improve security
  - City council voted to proceed

Surveillance and Community Safety Ordinance

"Surveillance Ordinance" passed May 2018

Ordinance adding Ch. 9.64 to the Municipal Code Establishing Rules For the City's Acquisition and Use of Surveillance Tech

- **Purpose:** Establish a public approval process for surveillance technologies used by the city; lay the groundwork for the City Council to decide whether the benefits of using the technology outweigh the costs to privacy.
- **City obligations:** City agencies must submit **a "technology impact report"** and a **use policy** to Oakland's Privacy Advisory Commission if they plan to implement new surveillance technologies, like license plate readers or cellphone trackers.
- **"Surveillance Technologies":** Any software, electronic device, system utilizing an electronic device, or similar used, designed, or primarily intended to collect, retain, analyze, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group.
- **Differentiated from other cities**: 1) Standardized public format for evaluation and approval; 2) Prohibits secret contracts or non-disclosure agreements between cities and third parties; 3) Provides whistleblower protections to employees who report violations.



How does the Surveillance Ordinance work in practice? Process for city to acquire or use a surveillance technology

Notification

- City entity **notifies** PAC Chair of its wish to acquire new surveillance technology.

Report Submission

- City entity submits a **Surveillance Impact Report** and proposed **Surveillance Use Policy** to the Privacy Advisory Commission for its review at a regularly noticed meeting.

PAC Evaluation

- PAC reviews documentation, works with City entity to revise Impact Report and Use Policy
- Recommends that the City Council **adopt**, **modify**, or **reject** the proposed Surveillance Use Policy.

Public Notice

- City Council provides **public notice** that will include the Surveillance Impact Report, proposed Surveillance Use Policy, and Privacy Advisory Commission recommendation at least fifteen (15) days prior to the public hearing.

Public Hearing

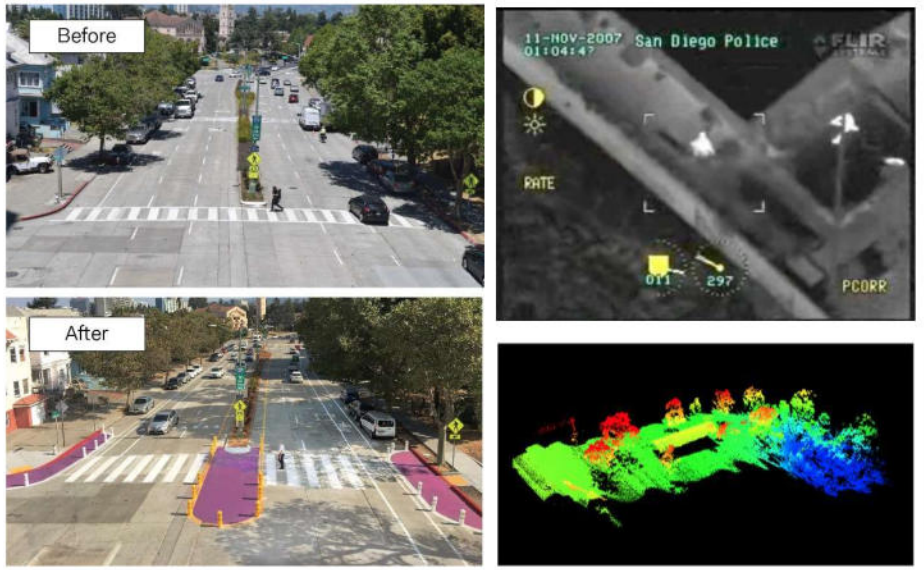
- City Council determination: 1) benefits to the community outweighs the costs; 2) proposal will safeguard civil liberties and civil rights; and 3) no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective.

Illustrative Examples

Types of requests include:

- DOT acquisition of **Unmanned Arial Vehicles (UAVs)** to document transportation improvement projects;
- DOT Parking and Mobility using vehicle-mounted **Automatic License Plate Recognition (ALPR)** to "virtually chalk" vehicles in time-limited spaces, verify permit parking, monitor "pay by phone" parking payments;
- District Attorney' use of **surveillance video** to monitor illegal dumping;
- Police Dept. use of **cell site simulators** to locate missing persons and apprehend fugitives;
- . . .

E.g., Pending DOT request:



- **Data types and sources:** Optical cameras, IR cameras, LIDAR, mapping software
- **Potential impacts:** Capturing PII without notice or consent; Enabling targeted voyeurism; Data use and retention uncertainties
- **Mitigations:** Deploy only in public and with notice where possible; obfuscate faces and license plates. Two-person team; focus must remain on project

Elements of the Required Documents

(Heart of the ordinance)

Surveillance Impact Report:

A. Description of the technology
B. Proposed use(s)
C. Location to be deployed
D. Impact on civil rights and liberties
E. Mitigations
F. Data types and sources
G. Data security
H. Fiscal cost(s)
I. Third-party dependence
J. Alternative methods
K. Track record

Surveillance Use Policy:

A. Purpose of the use
B. Authorized use(s)
C. Data collection
D. Data access
E. Data protection
F. Data retention
G. Public access
H. Third party data sharing
I. Training
J. Auditing and Oversight
K. Maintenance

Ongoing Oversight With Annual Reporting

Elements of the Report:

A. Description of How the Technology Was Used
B. Whether and How Often Data Was Shared With Outside Entities
C. A Breakdown of Where the Technology Was Installed or Used
D. A Summary of any Complaints Received
E. An Analysis of Whether the Use Policy Adequately Protected Civil Liberties
F. The Results of Any Internal Audits
G. Information About Any Data Breaches, and Responses thereto
H. Crime Statistics That Help The Community Assess Efficacy
I. Total Costs, Both Upfront and Ongoing

(2) Researching City-wide Privacy Principles

- Design And Use Equitable Privacy Practices
- Limit Collection And Retention Of Personal Information
- Manage Personal Information With Diligence
- Extend Privacy Protections To Our Relations With 3rd Parties
- Safeguard Individual Privacy In Public Records Disclosures
- Be Transparent And Open
- Be Accountable to Residents

Questions?
Interested in engaging?

Please reach out!
We'd love to
hear from you.

brian@secure-justice.org

@b_haddy

@SecureJustice

SECURE JUSTICE

September 2020

OAKLAND'S PRIVACY ADVISORY COMMISSION

History, Process, and Next Steps

Brian Hofer

Executive Director, Secure Justice

Chair, City of Oakland's Privacy Advisory Commission

The Opportunity

Oakland contemplated building-out a multi-faceted surveillance apparatus

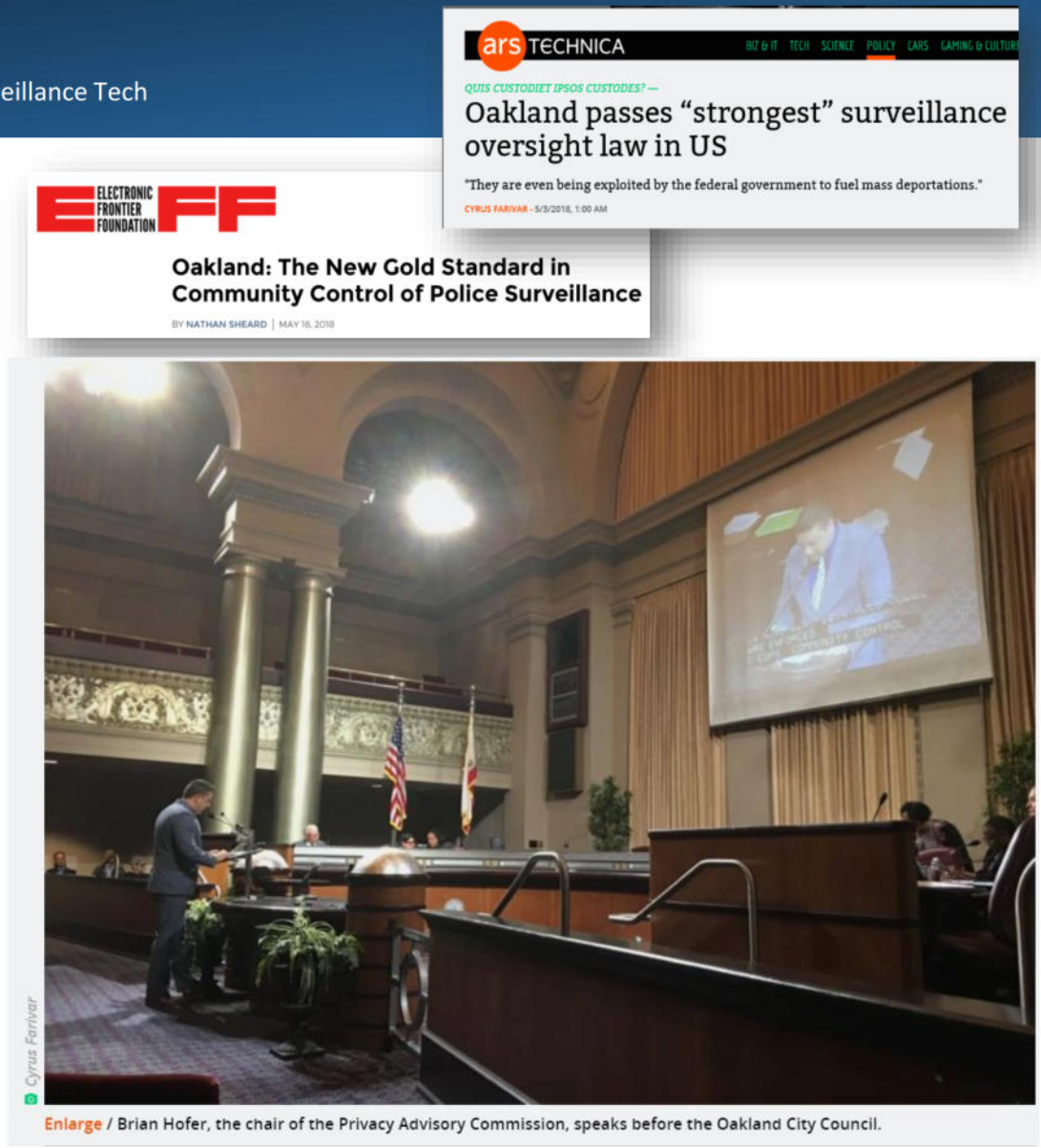
- In 2013, Oakland was given the opportunity to expand its Port's **Domain Awareness Center**
  - DHS would foot the $10.9M bill to build out a city-wide surveillance apparatus to fight terrorism and improve security
  - City council voted to proceed

Surveillance and Community Safety Ordinance

"Surveillance Ordinance" passed May 2018

Ordinance adding Ch. 9.64 to the Municipal Code Establishing Rules For the City's Acquisition and Use of Surveillance Tech

- **Purpose:** Establish a public approval process for surveillance technologies used by the city; lay the groundwork for the City Council to decide whether the benefits of using the technology outweigh the costs to privacy.
- **City obligations:** City agencies must submit **a "technology impact report"** and a **use policy** to Oakland's Privacy Advisory Commission if they plan to implement new surveillance technologies, like license plate readers or cellphone trackers.
- **"Surveillance Technologies":** Any software, electronic device, system utilizing an electronic device, or similar used, designed, or primarily intended to collect, retain, analyze, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group.
- **Differentiated from other cities**: 1) Standardized public format for evaluation and approval; 2) Prohibits secret contracts or non-disclosure agreements between cities and third parties; 3) Provides whistleblower protections to employees who report violations.



How does the Surveillance Ordinance work in practice? Process for city to acquire or use a surveillance technology

Notification

- City entity **notifies** PAC Chair of its wish to acquire new surveillance technology.

Report Submission

- City entity submits a **Surveillance Impact Report** and proposed **Surveillance Use Policy** to the Privacy Advisory Commission for its review at a regularly noticed meeting.

PAC Evaluation

- PAC reviews documentation, works with City entity to revise Impact Report and Use Policy
- Recommends that the City Council **adopt**, **modify**, or **reject** the proposed Surveillance Use Policy.

Public Notice

- City Council provides **public notice** that will include the Surveillance Impact Report, proposed Surveillance Use Policy, and Privacy Advisory Commission recommendation at least fifteen (15) days prior to the public hearing.

Public Hearing

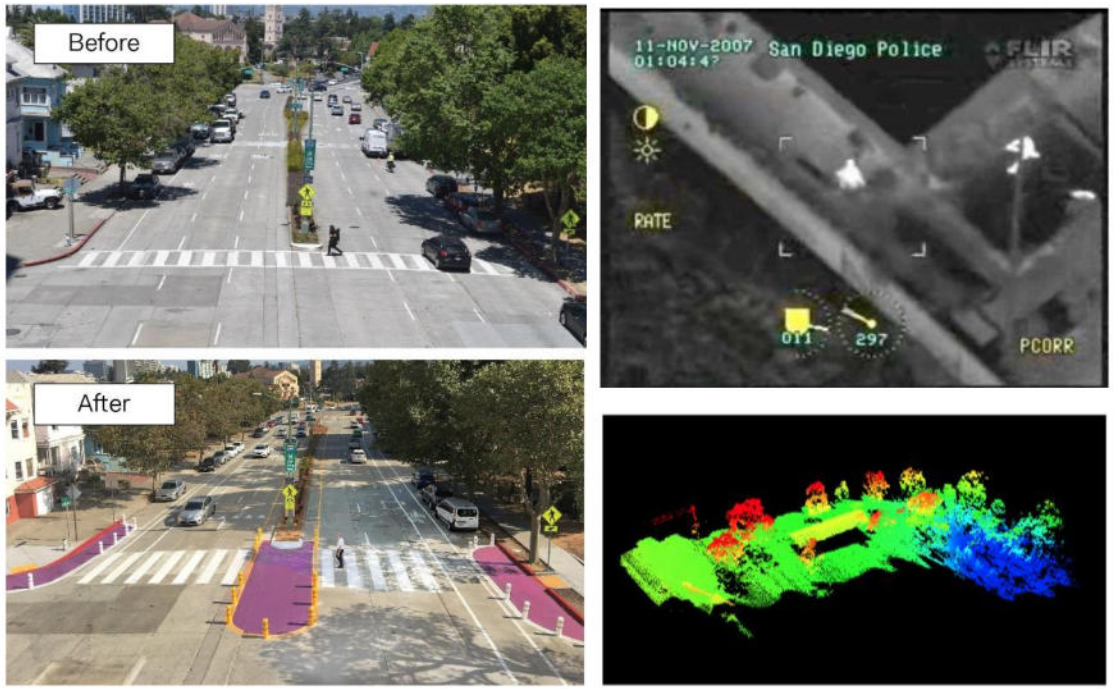
- City Council determination: 1) benefits to the community outweighs the costs; 2) proposal will safeguard civil liberties and civil rights; and 3) no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective.

Illustrative Examples

Types of requests include:

- DOT acquisition of **Unmanned Arial Vehicles (UAVs)** to document transportation improvement projects;
- DOT Parking and Mobility using vehicle-mounted **Automatic License Plate Recognition (ALPR)** to "virtually chalk" vehicles in time-limited spaces, verify permit parking, monitor "pay by phone" parking payments;
- District Attorney' use of **surveillance video** to monitor illegal dumping;
- Police Dept. use of **cell site simulators** to locate missing persons and apprehend fugitives;
- . . .

E.g., Pending DOT request:



- **Data types and sources:** Optical cameras, IR cameras, LIDAR, mapping software
- **Potential impacts:** Capturing PII without notice or consent; Enabling targeted voyeurism; Data use and retention uncertainties
- **Mitigations:** Deploy only in public and with notice where possible; obfuscate faces and license plates. Two-person team; focus must remain on project

Elements of the Required Documents

(Heart of the ordinance)

Surveillance Impact Report:

A. Description of the technology
B. Proposed use(s)
C. Location to be deployed
D. Impact on civil rights and liberties
E. Mitigations
F. Data types and sources
G. Data security
H. Fiscal cost(s)
I. Third-party dependence
J. Alternative methods
K. Track record

Surveillance Use Policy:

A. Purpose of the use
B. Authorized use(s)
C. Data collection
D. Data access
E. Data protection
F. Data retention
G. Public access
H. Third party data sharing
I. Training
J. Auditing and Oversight
K. Maintenance

Ongoing Oversight With Annual Reporting

Elements of the Report:

A. Description of How the Technology Was Used
B. Whether and How Often Data Was Shared With Outside Entities
C. A Breakdown of Where the Technology Was Installed or Used
D. A Summary of any Complaints Received
E. An Analysis of Whether the Use Policy Adequately Protected Civil Liberties
F. The Results of Any Internal Audits
G. Information About Any Data Breaches, and Responses thereto
H. Crime Statistics That Help The Community Assess Efficacy
I. Total Costs, Both Upfront and Ongoing

(2) Researching City-wide Privacy Principles

- Design And Use Equitable Privacy Practices
- Limit Collection And Retention Of Personal Information
- Manage Personal Information With Diligence
- Extend Privacy Protections To Our Relations With 3rd Parties
- Safeguard Individual Privacy In Public Records Disclosures
- Be Transparent And Open
- Be Accountable to Residents

Questions?
Interested in engaging?

Please reach out!
We'd love to
hear from you.

brian@secure-justice.org

@b_haddy

@SecureJustice

SECURE JUSTICE

SERGIO PEREZ

EDUCATION:

Yale Law School (New Haven, CT)
Juris Doctor, May 2010

University of California, Berkeley (Berkeley, CA)
B.A. in History and Political Science, May 2007
Phi Beta Kappa, Magna Cum Laude (High Distinction)

EXPERIENCE:

Executive Director, May 2020 to Present
Office of Independent Review, Orange County

- Lead the Office of Independent Review, an oversight and accountability body with authority over five justice-related county agencies: the District Attorney's Office, the Sheriff's Department, the Probation Department, the Public Defender's Office, and the Social Services Agency.
- Monitor and review specific incidents and systemic issues relating to high risk practices, including deaths, serious bodily injuries, and allegations of misconduct.
- Provide advice and legal counsel to the County Board of Supervisors on high-profile matters of public interest.
- Create and publish reports to educate the public and make necessary recommendations.
- Serve as liaison to stakeholder and community organizations.

Special Assistant and Constitutional Policing Advisor, November 2018 to May 2020
Office of the Inspector General, Los Angeles County

- Managed reviews of Los Angeles County juvenile justice system, and served as primary author of public reports, including 2019 report that led to the elimination of pepper spray in the County's juvenile halls and camps.
- Counseled the Inspector General and other executive staff on investigations, oversight, accountability, and related matters.
- Assisted in oversight of the Los Angeles County Sheriff's Department, including matters related to allegations of workplace discrimination.
- Developed and helped implement internal policies guiding investigations and audits.

Deputy Attorney General, June 2018 to November 2018
Office of the Attorney General, Civil Rights Enforcement Section, Cal. Dept. of Justice

- Investigated potential violations of federal and state civil rights statutes, with an emphasis on working with county and city law enforcement agencies to ensure lawful policing practices.
- Worked to execute reform agreement affecting the San Francisco Police Department's handling of allegations of discrimination and sexual harassment.
- Carried out collaborative review of Sacramento Police Department policies, practices, and investigations following the shooting of Stephon Clark, and helped author resulting public report assessing related practices and high-profile officer-involved shootings.

Director of Enforcement, August 2014 to June 2018
Los Angeles City Ethics Commission, Enforcement Division

- Led staff of attorneys and investigators assessing allegations of misconduct by City employees. Pursued landmark investigation of money laundering by member of the Los Angeles School Board, resulting in an unprecedented resignation and criminal plea.
- Served as first-chair litigator in all contested hearings and negotiations of enforcement

settlements.
- Managed the Ethics Commission's whistleblower hotline, and reviewed allegations of misconduct.
- Worked with community groups, City agencies, non-profits, and for-profit corporations to ensure compliance and support of good government laws.
- Developed proposed policies, regulations, City laws, and Charter modifications.
- Provided general legal counsel to Ethics Commission Executive Director, and developed ethics training.
- Presented all enforcement matters, including proposed settlements and policy issues, to members of the Los Angeles City Ethics Commission and administrative law judges.
- Led the development of litigation and investigation strategies, including legal research on novel issues related to relevant federal, state, and City ethics laws.

Enforcement Counsel, December 2013 to August 2014
Consumer Financial Protection Bureau, Office of Fair Lending & Equal Opportunity
- Worked with the Office of Fair Lending to investigate allegations of discriminatory practices by large national bank and non-bank corporations engaged in predatory lending.
- Formed and maintained relationships with various stakeholders in vulnerable communities affected by the work of the CFPB.
- Developed regulations affecting the financial practices of corporations in the transportation industry, including those engaged in automobile sales and lending to facilitate sales.
- Created processes and policies for a new federal agency, including Bureau-wide guidance and regulations.
- Led the development of litigation and investigation strategies related to the Equal Credit Opportunity Act.

Trial Attorney, September 2010 to December 2013
U.S. Department of Justice, Civil Rights Division, Special Litigation Section
- Engaged in high-profile, complex civil litigation and investigation of unconstitutional and discriminatory misconduct by law enforcement agencies as a trial attorney, including the United States' lawsuit against Sheriff Joseph Arpaio.
- Led of investigation of the Puerto Rico Police Department, one of the largest police forces in the United States, and worked to develop and enact a landmark consent decree.
- Mobilized immigrant and vulnerable communities in various jurisdictions across the country to identify potential legal claims.
- Conducted several depositions and authored and argued several pre-trial motions in federal court.
- Managed the receipt and review of voluminous document productions, interviewing witnesses, and worked with subject-matter experts, including statisticians.
- Conducted legislative and policy analyses related to proposed civil rights and immigration laws.
- Authored several complaints, settlement agreements, and consent decrees.

AWARDS: U.S. Department of Justice, Special Commendation Awards received in 2011, 2012, and 2013.

OTHER: Native/Fluent Spanish speaker and avid photographer.
Member, Executive Committee of the Yale Law School Association, 2010-2012
Student Director, Legal Services for Immigrant Communities Clinic, 2009-2010.
Co-Chair, Latino Law Students Association, 2008-2009.
Yale Law Coker Fellow, Assistant Instructor (Contracts – Prof. Robert Gordon), Fall 2009.

SURVEILLANCE ORDINANCE FACTS AS OF NOVEMBER 1, 2020

- Each of the seven existing California surveillance ordinances follows a similar approval process as the proposed San Diego ordinance. **The first six existing ordinances were adopted by unanimous vote of the governing body. The most recent** (San Francisco) **was adopted by a 10-1 vote.**
- Under this model, **no proposal has been permanently rejected** (several have been sent back to staff for additional analysis or draft policy amendments), and **no directive to cease use of existing equipment** has been issued[1]. What we are seeing in practice is that various stakeholders, including the general public and outside subject matter experts, provide feedback to the staff's proposed use policy which usually results in several amendments, before eventual and subsequent adoption by the governing board.
- As the first entity to adopt this model in the country (June 2016), Santa Clara County has had sufficient time to do a formal review of the ordinance. Only minor amendments were proposed in September 2018 (edits to several headings and re-arranging several sections for ease of reference). **No amendments to the framework or process were formally proposed by any department**. **No formal challenges to the governance structure have occurred. No department formally requested relief from compliance, nor requested additional staffing.** We have seen no evidence of an undue administrative burden or increased staffing costs in these seven jurisdictions[2].
- **No disciplinary action has occurred** under this model in the seven above jurisdictions pursuant to a complaint from a member of the public (or otherwise, to our knowledge), suggesting that staff is able to comply and that the heightened scrutiny and transparency around both the policy rules and equipment use is ensuring that operators stay within the approved guidelines.
- **Only one legal action has commenced** pursuant to the private right of action in the seven above jurisdictions, against suggesting that the model is pragmatic.
- **Outside of California,** nine jurisdictions have adopted similar surveillance ordinances. An additional twenty-one jurisdictions are working on or have formally introduced a similar model.[3]
- Oakland, San Francisco, Davis, and Berkeley each **involve a citizen's commission** in the ordinance vetting process[4].

[1] The bans on city use of facial recognition in San Francisco, Oakland, and Berkeley were not in response to a proposal.
[2] Santa Clara County has the most use policies of the seven jurisdictions, covering 77 types of technology. The average number of policies in the other 6 jurisdictions is approximately 10, although future Smart City proposals are expected to increase this number.
[3] https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance (last reviewed January 19, 2020)
[4] The Davis Police Commission is not incorporated into their surveillance ordinance. However, the commission has become part of the review process and amendments are in play that will likely formally incorporate them into the ordinance.

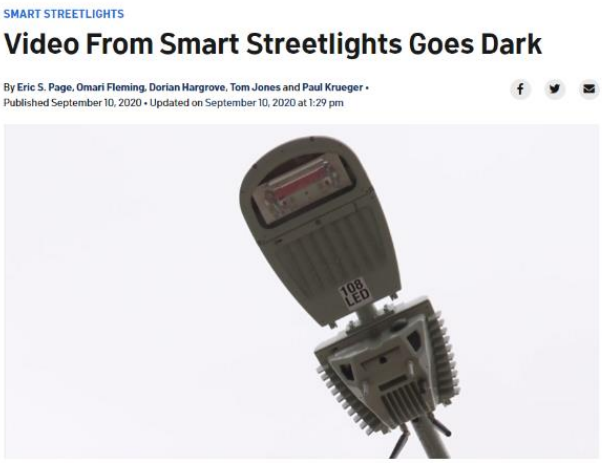
WHY DOES LOS ANGELES NEED THIS FRAMEWORK?

- Californians strongly support this kind of legislation. A March 2019 David Binder Research poll conducted by the ACLU of likely 2020 voters revealed that over 76% of likely statewide voters **support** having a vetting framework like that proposed by Council Member Montgomery and the Trust SD Coalition.

Three-quarters of voters statewide and in the Bay Area support a law to require public debate and a vote by lawmakers before any surveillance technology is obtained or used by government and law enforcement. Half of voters statewide and in the Bay Area *strongly* support this proposal.

Please tell support or oppose this proposal relating to limiting and requiring oversight for government and law enforcement surveillance. *Pass a law to require public debate and a vote by lawmakers before any surveillance technology is obtained or used by government and law enforcement.*				
	Statewide, Likely voters		**Bay Area, Likely Voters**	
Support, strongly	50%	→76%	51%	→76%
Support, Somewhat	26		25	
Oppose, Somewhat	9	→19%	7	→17%
Oppose, Strongly	10		10	
Don't know	5		7	

- In 2016, the City of San Diego rolled out what some are calling the largest installation of smart streetlights (capable of capturing video and audio, among other sources of data) in the world, telling taxpayers they could expect to save $2.8MM a year from lower energy costs. It was subsequently revealed that costs were double the projected amount, including an additional $1.1MM hit for unanticipated "operational costs" that were not considered during the vetting process, and that the expected energy savings were vastly overstated.[5]



[5] https://www.nbcsandiego.com/news/local/memo-reveals-huge-cost-overruns-for-san-diegos-smart-streetlights/2264320/

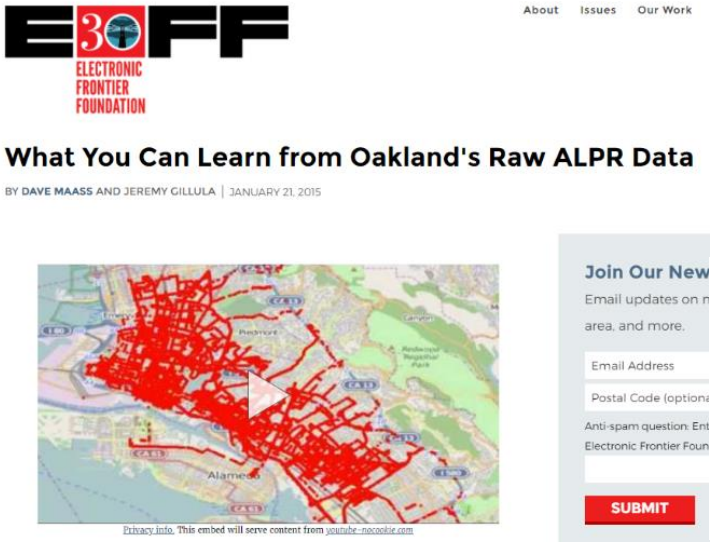
NBC 7 Investigates also reported on a Feb. 12 city memo which found the smart streetlight program would cost taxpayers millions more than expected.

In that memo, Erik Caldwell, the deputy chief operating officer for San Diego's Smart and Sustainable Communities Division revealed that the program suffered from a "lack of oversight," a failure to conduct "proper due diligence" and that city staff in charge of the program had "limited technological expertise."

Caldwell also said his department had uncovered "errors and missing information" in the program's accounting, revealing that his department found that the energy savings expected by converting to LED street lights were exaggerated by about $800,000 a year. City staff had used the energy savings as an incentive for the city council to approve entering into the initial contract for the streetlights.

In addition to the lower savings, Caldwell said there were hundreds of thousands of dollars in "unanticipated operational expenses," including $500,000 annually for a computer interface for each node, $140,000 a year for "data connectivity" and $446,000 for maintenance, data analysis and lighting issues.

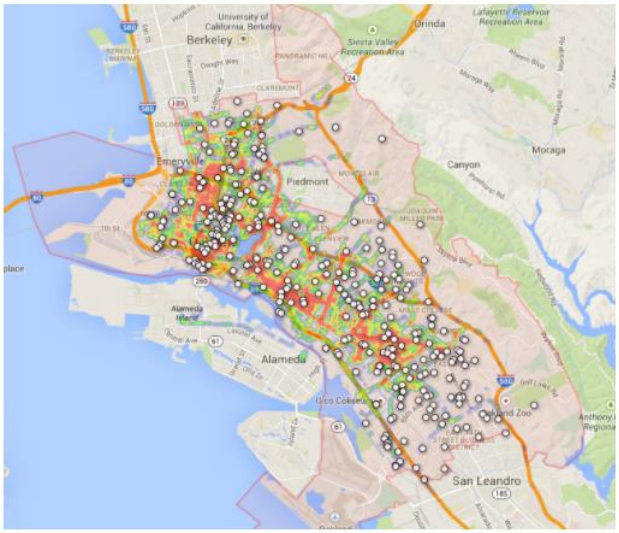
- Warrantless tracking of cellphone location data at a labor union protest, in the absence of any criminal predicate.[6]
- Oregon's Attorney General forced to publicly apologize after her department used software to target Twitter users that posted #BlackLivesMatter.[7]
- Third-party analysis of the Oakland Police Department's use of automated license plate readers revealed that even after controlling for property and automobile related crime, use disproportionately impacted African American [8]



Per Capita Income: The data indicates lower-income neighborhoods are disproportionately captured by ALPR patrols, with police vehicles creating a grid of license plates in the city's poorest neighborhoods.

[6] https://www.newsweek.com/fbi-tracks-suspects-cell-phones-without-warrant-75099
[7] https://www.reuters.com/article/us-oregon-race-idUSKCN0T104N20151112
[8] https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data

To see if perhaps OPD was just focusing its ALPR use in areas with high incidents of automobile-related crime, we decided to map only the auto-related crime:



The result is the same—ALPRs are clearly not being used to deter automobile-related crimes.

- After the Los Angeles Sheriff's secret aerial surveillance system over Compton was discovered, the residents and elected leaders of Compton became outraged, further causing distrust of law enforcement and the government.[9]
- The New York police department paid $2 million in attorney fees to settle civil rights lawsuits alleging baseless surveillance of the Muslim community. Stronger civilian oversight was created as part of the settlement.[10]
- Forty-seven-year-old African American Denise Green is pulled from her car and thrown on the ground by seven officers pointing their guns at her. The license plate reader that alerted the officers misread her plate by one digit, and no officers verified accuracy. The taxpayers of San Francisco paid Green $495,000.[11]

[9] https://www.latimes.com/local/lanow/la-me-ln-sheriffs-surveillance-compton-outrage-20140423-story.html
[10] https://www.washingtonpost.com/world/national-security/nypd-settles-lawsuits-over-muslim-monitoring/2016/01/07/bdc8eb98-b3dc-11e5-9388-466021d971de_story.html
[11] https://www.techdirt.com/articles/20140513/07404127218/another-bogus-hit-license-plate-reader-results-another-citizen-surrounded-cops-with-guns-out.shtml

The City is expected to settle a $495,000 lawsuit with a woman who claimed to be wrongfully arrested by police who thought she was driving a stolen car. (MIKE KOOZMIN/S.F. EXAMINER FILE PHOTO)

City set to approve wrongful arrest suit settlement

JOSHUA SABATINI / Sep. 7, 2015 12:00 a.m. / NEWS / THE CITY

About six years after San Francisco police officers placed a woman at gunpoint over wrongfully suspecting her of driving a stolen Lexus in the Mission, The City is expected to settle the lawsuit she filed for $495,000, city documents show.

Privacy advocate held at gunpoint after license plate reader database mistake, lawsuit alleges

The rental car was allegedly reported as stolen

Photo by Justin Sullivan/Getty Images

Bay Area police pulled over a California privacy advocate and held him at gunpoint after a database error caused a a license plate reader to flag a car as stolen, a lawsuit alleges.

Brian Hofer, chair of Oakland's Privacy Advisory Commission, said in a suit filed in December that he had rented a car and was traveling with his brother in November when he was pulled over by a Contra Costa Sheriff's Office deputy, and more police cars joined. Hofer alleges that an officer had a gun drawn and told him and his brother to exit the rental car, and that a deputy injured his brother by throwing him to the ground.

Some of the best Nintendo Switch games are discounted today

[12]

- After spending hundreds of hours of valuable staff time planning a city-wide surveillance system in secret from 2008-2013, the City Council of Oakland was forced to dramatically scale back the project due to public outrage after the item was finally presented at a public hearing. Millions of dollars in federal grant money and staff time was squandered.[13]
- After secretly applying for federal grant money and acquiring a drone, the San Jose police department was forced to publicly apologize to the public when the drone was discovered, subsequently promising greater transparency and community input into use before the drone might be used.[14]
- More than 2,000 cases could be overturned in Baltimore due to an alleged conspiracy between the state's attorney and police department to withhold discovery evidence pertaining to use of a Stingray cellphone tracking device from defense counsel.[15]
- An audit of Walnut Creek, CA's use of red-light traffic enforcement cameras revealed that the use of the technology led to a dramatic increase in rear-end collisions (71%) and broadside collisions (100%), finding that the "use of red light cameras appears to have decreased safety and put roadway users at increased risk.[16]
- Saying that the police need to focus on community building, City of Seattle Mayor pulls plug on controversial secret drone program before it even begins, due to community concerns after the plan was discovered.[17]

For more information: https://www.aclunc.org/docs/20160325-making_smart_decisions_about_surveillance.pdf

BENEFITS TO PARTICIPATING IN A SURVEILLANCE EQUIPMENT & PRIVACY COMMISSION VETTING FRAMEWORK

Each of the problems that the surveillance ordinance (by itself) is expected to solve, will still remain if Los Angeles does not also incorporate the Police Commission into the vetting framework to make recommendations to the City Council. A surveillance ordinance by itself will not create more capacity for research or greater understanding by elected city council members, nor will it ensure that those same electeds become surveillance

[12] https://www.theverge.com/2019/2/21/18234785/privacy-advocate-lawsuit-california-license-plate-reader
[13] https://www.sfgate.com/bayarea/article/Oakland-to-limit-surveillance-center-to-port-5290273.php#
[14] https://www.mercurynews.com/2014/08/05/san-jose-police-apologize-for-drone-secrecy-promise-transparency/
[15] https://www.theguardian.com/us-news/2015/sep/04/baltimore-cases-overturned-police-secret-stingray-surveillance
[16] https://www.dailynews.com/2014/01/21/red-light-cameras-being-stopped/
[17] https://www.seattletimes.com/seattle-news/seattle-grounds-police-drone-program/

technology or privacy law experts. A public review process at the commission also provides for more public input, greater transparency, and more collaboration with city staff. In Oakland, the Privacy Advisory Commission's endorsement of potentially controversial equipment has provided comfort to both the public and city council that the technology was properly vetted, and that appropriate guardrails were put into place in the corresponding use policy.

"As a long-time resident of Oakland, I understood the intent and recognized the importance of the City's Privacy Advisory Commission's (PAC) proposed surveillance vetting ordinance, so much so that I showed up and expressed strong support when the City Council considered and then adopted it. As a manager in Oakland's Department of Transportation responsible for over a dozen parking and mobility programs that all use various types of technology with clear or possible surveillance capabilities, I have gone through the PAC's process on a number of occasions and believe that the model is delivering on its promises.

For example, I appreciate that the surveillance ordinance required topics of discussion that prompt myself, my staff and our vendors to address areas we might have overlooked, and the feedback we receive from the Commissioner's on our proposed use policies has been most helpful. Additionally, the framework afforded by the ordinance clearly helped our proposals sail through the City Council with unanimous votes, this after we received the PAC's endorsement and further instilling confidence in our work. Once newly procured technologies have been implemented, the PAC approved use policies have proven to be a touchstone for guiding our work and responding to questions or concerns from the community or responding to requests from other departments or agencies. As a result, I now recognize the work that goes into meeting staff's obligations under the City's surveillance ordinance is most welcome as it protects privacy and builds trust and confidence in staff's work while improving efficiencies. This was entirely unexpected but most welcomed!" - *Michael Ford, Manager – Parking & Mobility Division, City of Oakland Department of Transportation*

Especially in 2020, when trust in law enforcement is at an all-time low and people all across the country are demanding that we "reimagine public safety", it is critical that the police participate in the public review process and collaborate with the Police Commission to repair relationships, provide greater transparency into the use of powerful technology, and regain the public's trust with hopefully demonstrated good behavior via the annual reporting mechanism.

"It goes without saying that change can be difficult to achieve for large organizations. However, working alongside the Privacy Advisory Commission and its Commissioners, I have seen positive change occur. The Privacy Commission and the Oakland Police Department collaborate in a transparent process that aims to both protect the civil liberties of Oakland community members and increase understanding about the need to use technology in a responsible manner to provide public safety. The Privacy Commission and the Department together work toward improving public trust by providing a platform that allows for the opportunity to dispel rumors or suspicions about technology used in modern policing, identification of potential impact to the community from using the technology, and monitoring the overall effectiveness of the technology. Although change can be difficult, the Department welcomes the opportunity to continue to work collectively with the Privacy Commission to make Oakland a city safer for all." - *Deputy Chief Roland Holmgren, City of Oakland Police Department*

"Oakland was a very different place in 2013, when we submitted the Domain Awareness Center proposal for City Council approval. We had no privacy policies in place, and with Edward Snowden dominating the news, the project understandably tapped into the public's fear around mass surveillance and unfettered data sharing. The creation of the Privacy Commission in 2015 was one of the smartest things the City of Oakland has done -

it's led to greater trust in law enforcement and created a culture of "mindfulness" in the staff, so that we think about the potential impact before putting surveillance technology out into the wild.

"As Chief Privacy Officer for the City of Oakland, and liaison between the City Administrator and the Privacy Commission, I've had a front row seat to watching the interaction between various city departments and the commissioners as they vet surveillance technology together. The benefits to such a framework are becoming readily apparent, and the City Council has easily and unanimously approved each recommendation put forth by the commission. I feel that the commissioners have done a good job deferring to city staff when appropriate, while still ensuring that they defend the civil liberties and privacy interests of Oaklanders." - *Joe DeVries, City of Oakland Chief Privacy Officer and Assistant to the City Administrator*

> **The public vetting and information supplied in the required up-front analysis will help dispel rumors and conspiracy theories, leading to greater community trust and input.**

“From my perspective, the process itself is fine and I don’t really have any issues. So far council has approved most of what we’ve asked for and to them we accomplished what the real goal was, which was to disclose what we do have, and by default what we don’t have.” - *Chief Darren Pytel, City of Davis Police Department*

THE SURVEILLANCE AND COMMUNITY SAFETY ORDINANCE

Whereas, the City Council finds it is essential to have an informed public debate as early as possible about decisions related to surveillance technology; and

Whereas, the City Council finds that, while surveillance technology may threaten the privacy of all citizens, throughout history, surveillance efforts have been used to intimidate and oppress certain communities and groups more than others, including those that are defined by a common race, ethnicity, religion, national origin, income level, sexual orientation, or political perspective; and

Whereas, the City Council finds that surveillance technology may also be a valuable tool to bolster community safety and aid in the investigation and prosecution of crimes, while acknowledging the significance of protecting the privacy of citizens; and

Whereas, the City Council finds that surveillance technology includes not just technology capable of accessing non-public places or information (such as wiretaps) but also technology which aggregates publicly available information, because such information, in the aggregate or when pieced together with other information, has the potential to reveal a wealth of detail about a person's familial, political, professional, religious, or sexual associations; and

Whereas, the City Council finds that no decisions relating to surveillance technology should occur without strong consideration being given to the impact such technologies may have on civil rights and civil liberties, including those rights guaranteed by the California and United States Constitutions; and

Whereas, the City Council finds that any and all decisions regarding if and how surveillance technologies should be funded, acquired, or used should include meaningful public input and that public opinion should be given significant weight; and

Whereas, the City Council finds that legally enforceable safeguards, including robust transparency, oversight, and accountability measures, must be in place to protect civil rights and civil liberties before any surveillance technology is deployed; and

Whereas, the City Council finds that if a surveillance technology is approved, data reporting measures must be adopted that empower the City Council and public to verify that mandated civil rights and civil liberties safeguards have been strictly adhered to; now, therefore

THE CITY COUNCIL OF THE CITY OF LOS ANGELES DOES ORDAIN AS FOLLOWS:

Section 1. Title

This ordinance shall be known as the Surveillance & Community Safety Ordinance.

Section 2. City Council Approval Requirement

1) The Police Department shall notify the President of the Police Commission prior to:
    a) Seeking or soliciting funds for new surveillance technology or to replace existing surveillance technology that has not been previously approved by the City Council pursuant to the requirements of this Ordinance, including but not limited to applying for a grant; or,
    b) Soliciting proposals with a non-City entity to acquire, share or otherwise use surveillance technology or the information it provides.

    Upon notification by the Police Department, the President shall place the item on the agenda at the next meeting for discussion and possible action. At this meeting, the Police Department shall inform the Police Commission of the need for the funds or equipment or shall otherwise justify the action the Police Department intends to take. The Police Commission may vote its approval to proceed, object to the proposal, recommend that the Police Department modify its proposal, or take no action. Failure by the Police Commission to act shall not prohibit the Police Department from proceeding. Opposition to the action by the Police Commission shall not prohibit the Police Department from proceeding. The Police Department is still bound by subsection (2) regardless of the action taken by the Police Commission under this subsection.

2) The Police Department must obtain City Council approval, subsequent to a mandatory, properly noticed, germane, public hearing prior to any of the following:

A. Accepting state or federal funds or in-kind or other donations for surveillance technology, except for surveillance technology that has a City Council approved corresponding use policy in effect;

B. Acquiring new surveillance technology, or replacing existing surveillance technology that has not been previously approved by the City Council pursuant to the requirements of this Ordinance, including but not limited to procuring such technology without the exchange of monies or consideration;

C. Using new surveillance technology, or using existing surveillance technology or the information it provides for a purpose, in a manner, or in a location not previously approved by the City Council pursuant to the requirements of this Ordinance, except that for surveillance technology that has been acquired or is in use prior to enactment of this Ordinance, such use may continue until the City Council votes to approve or reject the surveillance technology's corresponding use policy; or

D. Entering into an agreement with a non-City entity to acquire, share or otherwise use surveillance technology or the information it provides, including data sharing arrangements.

3) The Police Department must obtain City Council approval of a Surveillance Use Policy prior to engaging in any of the activities described in subsection (2)(a)-(d).

Section 3. Information Required

1) When seeking approval under Section 2, the Police Department shall submit to the City Council a Surveillance Impact Report and a proposed Surveillance Use Policy. A Surveillance Use Policy shall be considered a draft proposal until such time as it is approved pursuant to a vote of the City Council.
    a) Prior to seeking City Council approval under Section 2, the Police Department shall submit the Surveillance Impact Report and proposed Surveillance Use Policy to the Police Commission for its review at a regularly noticed meeting.
    b) The Police Commission shall recommend that the City Council adopt, modify, or reject the proposed Surveillance Use Policy. If the Police Commission proposes that the Surveillance Use Policy be modified, the Police Commission shall propose modifications to the Police Department and/or City Council in writing.
    c) Failure by the Police Commission to make its recommendation on the item within 90 days of submission shall enable the Police Department to proceed to the City Council for approval of the item.
2) After receiving the recommendation of the Police Commission, the City Council shall provide the public notice that will include the Surveillance Impact Report, proposed Surveillance Use Policy, and Police Commission recommendation at least fifteen (15) days prior to the public hearing. The Police Department shall not unreasonably delay scheduling any item for City Council consideration at the next earliest opportunity.
3) The City Council, or its appointed designee, shall continue to make the Surveillance Impact Report and Surveillance Use Policy, and updated versions thereof, available to the public as long as the Police Department continues to utilize the surveillance technology in accordance with its request pursuant to Section 2(1).

Section 4. Determination by City Council that Benefits Outweigh Costs and Concerns

The City Council shall only approve any action described in Section 2, subsection (1) or Section 5 of this ordinance after first considering the recommendation of the Police Commission, and subsequently making a determination that the benefits to the community of the surveillance technology outweigh the costs; that the proposal will

safeguard civil liberties and civil rights; and that, in the City Council's judgment, no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective.

Section 5. Compliance for Existing Surveillance Technology

Upon adoption of this ordinance, the Police Department shall submit a Surveillance Impact Report and a proposed Surveillance Use Policy for each surveillance technology in use or possessed by the Police Department, in compliance with Section 3 (1) (a-c).

a) Prior to submitting the Surveillance Impact Report and proposed Surveillance Use Policy as described above, the Police Department shall present to the Police Commission a list of surveillance technology already possessed or in use by the department.
b) The Police Commission shall rank the items in order of potential impact to civil liberties.
c) Within sixty (60) days of the Police Commission's action in b), the Police Department shall submit at least one (1) Surveillance Impact Report and proposed Surveillance Use Policy per month to the Police Commission for review, beginning with the highest-ranking items as determined by the Police Commission, and continuing thereafter every month until the list is exhausted.
d) Failure by the Police Commission to make its recommendation on any item within 90 days of submission shall enable the Police Department to proceed to the City Council for approval of the item pursuant to Section 4. If such review and approval has not occurred within sixty (60) days of the City Council submission date, the Police Department shall cease its use of the surveillance technology until such review and approval occurs.

Section 6. Oversight Following City Council Approval

1) On April 30th of each year, or at the next closest regularly scheduled Police Commission meeting, city staff must present a written surveillance annual report for Police Commission review for each approved surveillance technology item. If the Police Department is unable to meet the deadline, they shall notify the Police Commission in writing of the department's request to extend this period, and the reason(s) for that request. The Police Commission may grant a single extension of up to sixty (60) days to comply with this provision.

A. After review by the Police Commission, the Police Department shall submit the surveillance annual report to the City Council.

B. The Police Commission shall recommend to the City Council that the benefits to the community of the continued use of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded; that use of the surveillance

technology cease; or propose modifications to the corresponding surveillance use policy that will resolve the concerns.

C. Failure by the Police Commission to make its recommendation on the item within ninety (90) days of submission shall enable the Police Department to proceed to the City Council for approval of the surveillance annual report.

2. Based upon information provided in the Police Department's surveillance annual report and after considering the recommendation of the Police Commission, the City Council shall re-visit its "cost benefit" analysis as provided in Section 4 and either uphold or set aside the previous determination. Should the City Council set aside its previous determination, the City's use of the surveillance technology must cease. Alternatively, the City Council may require modifications to the Surveillance Use Policy that will resolve any deficiencies.

Section 7. Definitions

The following definitions apply to this Ordinance:

1) "City" means the City of Los Angeles.
2) "Exigent Circumstances" means the Police Department's good faith belief that an emergency involving danger of, or imminent threat of death or serious physical injury to any person requires the use of surveillance technology or the information it provides.
3) "Personal Communication Device" means a mobile telephone, a personal digital assistant, a wireless capable tablet and a similar wireless two-way communications and/or portable internet accessing devices, whether procured or subsidized by a city entity or personally owned, that is used in the regular course of city business.
4) "Police Department" means the police department of the City of Los Angeles.
5) "Surveillance Annual Report" means a written report concerning a specific surveillance technology that includes all the following:
    a) A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology;
    b) Whether and how often data acquired through the use of the surveillance technology was directly shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);
    c) Where applicable, a breakdown of what physical objects the surveillance technology software was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to;
    d) Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area;

e) A summary of community complaints or concerns about the surveillance technology, and an analysis of the surveillance technology's adopted use policy and whether it is adequate in protecting civil liberties and civil rights. The analysis shall identify the race of each person that was subject to the technology's use. The Police Commission may determine, on an individual basis, to waive the obligation to identify the race of each person if the probative value is outweighed by the administrative burden and potential greater invasiveness in capturing such data. If the Police Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review;
f) The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel information;
g) Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response;
h) Information, including crime statistics, that help the community assess whether the surveillance technology has been effective at achieving its identified purposes;
i) Statistics and information about public records act requests;
j) Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year; and
k) Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.

6) "Surveillance technology" means any software, electronic device, technological tool, system utilizing an electronic device, or similar used, designed, or primarily intended to collect, retain, analyze, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group. Examples of surveillance technology include, but is not limited to the following: cell site simulators (Stingrays); automatic license plate readers; gunshot detectors (ShotSpotter); facial recognition software; thermal imaging systems; body-worn cameras; social media analytics software; gait analysis software; video cameras that record audio or video, and transmit or can be remotely accessed. It also includes software designed to monitor social media services or forecast criminal activity or criminality, and biometric identification hardware or software.

"Surveillance technology" does not include the following devices or hardware, unless they have been equipped with, or are modified to become or include, a surveillance technology as defined in Section 7(3):

A. Routine office hardware, such as televisions, computers, credit card machines, badge readers, copy machines, and printers, that is in widespread use and will not be used for any surveillance or law enforcement functions;

B. Parking Ticket Devices (PTDs);

C. Manually operated, non-wearable, handheld digital cameras, audio recorders, and video recorders that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings;

D. Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles;

E. Manually operated technological devices used primarily for internal municipal entity communications and are not designed to surreptitiously collect surveillance data, such as radios and email systems;

F. City databases that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology, including payroll, accounting, or other fiscal databases.

G. Medical equipment used to diagnose, treat, or prevent disease or injury.

H. Police department interview room cameras.

I. Police department case management systems.

J. Police department early warning systems.

K. Personal communication devices that have not been modified beyond stock manufacturer capabilities in a manner described above, provided that any bundled biometric technology is only used for the sole purpose of user authentication in the regular course of conducting City business.

7) “Surveillance Impact Report” means a publicly released written report including at a minimum the following:
    a) **Description:** Information describing the surveillance technology and how it works, including product descriptions and manuals from manufacturers.
    b) **Purpose:** Information on the proposed purposes(s) for the surveillance technology;
    c) **Location:** The location(s) it may be deployed, using general descriptive terms, and crime statistics for any location(s);
    d) **Impact:** An assessment of the technology's proposed use policy and whether it is adequate in protecting civil rights and liberties and whether the surveillance technology could be used or deployed, intentionally or inadvertently, in a manner that is discriminatory, viewpoint-based, or biased via algorithm;

e) **Mitigations:** Identify specific, affirmative technical and procedural measures that will be implemented to safeguard the public from each such impacts;
f) **Data Types and Sources:** A list of all types and sources of data to be collected, analyzed, or processed by the surveillance technology, including “open source” data, scores, reports, logic or algorithm used, and any additional information derived therefrom;
g) **Data Security:** Information about the steps that will be taken to ensure that adequate security measures are used to safeguard the data collected or generated by the technology from unauthorized access or disclosure;
h) **Fiscal Cost:** The fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, the operative or proposed contract, and any current or potential sources of funding;
i) **Third Party Dependence:** Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis;
j) **Alternatives:** A summary of all alternative methods (whether involving the use of a new technology or not) considered before deciding to use the proposed surveillance technology, including the costs and benefits associated with each alternative and an explanation of the reasons why each alternative is inadequate; and,
k) **Track Record:** A summary of the experience (if any) other entities, especially government entities, have had with the proposed technology, including, if available, quantitative information about the effectiveness of the proposed technology in achieving its stated purpose in other jurisdictions, and any known adverse information about the technology (such as unanticipated costs, failures, or civil rights and civil liberties abuses).

8) "Surveillance Use Policy" means a publicly-released and legally-enforceable policy for use of the surveillance technology that at a minimum specifies the following:
a) **Purpose:** The specific purpose(s) that the surveillance technology is intended to advance;
b) **Authorized Use:** The specific uses that are authorized, and the rules and processes required prior to such use;
c) **Data Collection:** The information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including “open source” data;
d) **Data Access:** The category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information;

e) **Data Protection:** The safeguards that protect information from unauthorized access, including encryption and access control mechanisms;
f) **Data Retention:** The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period;
g) **Public Access:** How collected information can be accessed or used by members of the public, including criminal defendants;
h) **Third Party Data Sharing:** If and how other City departments or non-City entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information;
i) **Training:** The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, and the identity of the category of staff that will provide the training;
j) **Auditing and Oversight:** The mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy; and
k) **Maintenance:** The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

9) "Surveillance" or "Surveil" means to observe or analyze the movements, behavior, data, or actions of individuals. Individuals include those whose identity can be revealed by license plate data when combined with any other record.

Section 8. Enforcement

1) Any violation of this Ordinance, or of a Surveillance Use Policy promulgated under this Ordinance, constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in any court of competent jurisdiction to enforce this Ordinance. An action instituted under this paragraph shall be brought against the respective city agency, the City of Los Angeles, and, if necessary to effectuate compliance with this Ordinance or a Surveillance Use Policy (including to expunge information unlawfully collected, retained, or shared thereunder), any third-party with possession, custody, or control of data subject to this Ordinance.

2) Any person who has been subjected to a surveillance technology in violation of this Ordinance, or about whom information has been obtained, retained, accessed, shared, or used in violation of this Ordinance or of a Surveillance Use Policy promulgated under this Ordinance, may institute proceedings in any court of competent jurisdiction against any person who committed such violation and shall be entitled to recover actual damages (but not less than liquidated damages of $1,000 or $100 per day for each day of violation, whichever is greater) and punitive damages.

3) A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought under paragraphs (1) or (2).

Section 9. Use of unapproved technology during exigent circumstances.

1. The Police Department may temporarily acquire or use surveillance technology and the data derived from that use in a manner not expressly allowed by a surveillance use policy without following the provisions of Sections 2-3.

2. If the Police Department acquires or uses a surveillance technology pursuant to subdivision 1, the Police Department shall:

A. Use the surveillance technology to solely respond to the exigent circumstances;

B. Cease using the surveillance technology when the exigent circumstances ends;

C. Only keep and maintain data related to the exigent circumstances and dispose of any data that is not relevant to an ongoing investigation unless otherwise required by law;

D. Following the end of the exigent circumstances, report that acquisition or use to the Police Commission at their next regularly scheduled meeting for discussion and/or possible recommendation to the City Council;

3. Any technology temporarily acquired in exigent circumstances shall be returned within seven (7) days following its acquisition, or when the exigent circumstances end, whichever is sooner, unless the technology is submitted to the City Council for approval pursuant to Section 2 and is approved. If the Police Department is unable to comply with the seven-day timeline, the Police Department shall notify the City Council, who may grant an extension.

Section 10. Secrecy of Surveillance Technology

It shall be unlawful for the City of Los Angeles or its Police Department to enter into any contract or other agreement that conflicts with the provisions of this Ordinance, and any conflicting provisions in such contracts or agreements, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable. To the extent permitted by law, the City of Los Angeles shall publicly disclose all of its surveillance-

related contracts, including any and all related non-disclosure agreements, if any, regardless of any contract terms to the contrary.

Section 11. Severability

The provisions in this Ordinance are severable. If any part of provision of this Ordinance, or the application of this Ordinance to any person or circumstance, is held invalid, the remainder of this Ordinance, including the application of such part or provisions to other persons or circumstances, shall not be affected by such holding and shall continue to have force and effect.

Section 12. Construction

The provisions of this Ordinance, including the terms defined in Section 7, are to be construed broadly so as to effectuate the purposes of this Ordinance.

Section 13. Effective Date

This Ordinance shall take effect on [DATE].