CITY OF OAKLAND

Privacy Advisory Commission

December 2, 2021 5:00 PM
Teleconference
Meeting Agenda

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian Hofer, Chair, **District 4 Representative**: Lou Katz, **District 5 Representative**: Omar De La Cruz, **District 6 Representative**: Gina Tomlinson, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Henry Gage III, Vice Chair **Mayoral Representative**: Vacant*

Pursuant to California Government Code section 54953(e), Oakland Privacy Advisory Commission Board Members/Commissioners, as well as City staff, will participate via phone/video conference, and no physical teleconference locations are required.

TO OBSERVE:
Please click the link below to join the webinar:
https://us02web.zoom.us/j/85817209915
Or iPhone one-tap:
US: +16699009128, 85817209915# or +13462487799, 85817209915#
Or Telephone:
Dial (for higher quality, dial a number based on your current location):
US: +1 669 900 9128 or +1 346 248 7799 or +1 253 215 8782 or +1 646 558 8656
Webinar ID: 858 1720 9915
International numbers available: https://us02web.zoom.us/u/kDUn0z2rP

TO COMMENT:
1) To comment by Zoom video conference, you will be prompted to use the “Raise Your Hand” button to request to speak when Public Comment is being taken on the eligible Agenda item. You will then be unmuted, during your turn, and allowed to make public comments. After the allotted time, you will then be re-muted.

2) To comment by phone, you will be prompted to “Raise Your Hand” by pressing “* 9” to request to speak when Public Comment is being taken on the eligible Agenda Item. You will then be unmuted, during your turn, and allowed to make public comments. After the allotted time, you will then be re-muted.
ADDITIONAL INSTRUCTIONS:
1) Instructions on how to join a meeting by video conference is available at: https://support.zoom.us/hc/en-us/articles/201362193%20-%20Joining-a-Meeting#
2) Instructions on how to join a meeting by phone are available at: https://support.zoom.us/hc/en-us/articles/201362663%20Joining-a-meeting-by-phone
3) Instructions on how to “Raise Your Hand” is available at: https://support.zoom.us/hc/en-us/articles/205566129-Raising-your-hand-In-a-webinar

1. Call to Order, determination of quorum

2. Adopt a Renewal Resolution regarding AB 361 establishing certain findings justifying the ongoing need for virtual meetings

3. Review and approval of the draft November meeting minutes

4. Open Forum/Public Comment

5. Surveillance Equipment Ordinance – DPW – Illegal Dumping Camera Proposal
    a. Review and take possible action on Impact Report and proposed Use Policy

OAKLAND PRIVACY ADVISORY COMMISSION

RESOLUTION NO. __2____________

ADOPT A RESOLUTION DETERMINING THAT CONDUCTING IN-PERSON MEETINGS OF THE PRIVACY ADVISORY COMMISSION AND ITS COMMITTEES WOULD PRESENT IMMINENT RISKS TO ATTENDEES' HEALTH, AND ELECTING TO CONTINUE CONDUCTING MEETINGS USING TELECONFERENCING IN ACCORDANCE WITH CALIFORNIA GOVERNMENT CODE SECTION 54953(e), A PROVISION OF AB-361.

WHEREAS, on March 4, 2020, Governor Gavin Newsom declared a state of emergency related to COVID-19, pursuant to Government Code Section 8625, and such declaration has not been lifted or rescinded. *See* https://www.gov.ca.gov/wp-content/uploads/2020/03/3.4.20-Coronavirus-SOE-Proclamation.pdf; and

WHEREAS, on March 9, 2020, the City Administrator in their capacity as the Director of the Emergency Operations Center (EOC), issued a proclamation of local emergency due to the spread of COVID-19 in Oakland, and on March 12, 2020, the City Council passed Resolution No. 88075 C.M.S. ratifying the proclamation of local emergency pursuant to Oakland Municipal Code (O.M.C.) section 8.50.050(C); and

WHEREAS, City Council Resolution No. 88075 remains in full force and effect to date; and

WHEREAS, the Centers for Disease Control (CDC) recommends physical distancing of at least six (6) feet whenever possible, avoiding crowds, and avoiding spaces that do not offer fresh air from the outdoors, particularly for people who are not fully vaccinated or who are at higher risk of getting very sick from COVID-19. *See* https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/prevention.html; and

WHEREAS, the CDC recommends that people who live with unvaccinated people avoid activities that make physical distancing hard. *See* https://www.cdc.gov/coronavirus/2019-ncov/your-health/about-covid-19/caring-for-children/families.html; and

WHEREAS, the CDC recommends that older adults limit in-person interactions as much as possible, particularly when indoors. *See* https://www.cdc.gov/aging/covid19/covid19-older-adults.html; and

WHEREAS, the CDC, the California Department of Public Health, and the Alameda County Public Health Department all recommend that people experiencing COVID-19 symptoms stay home. *See* https://www.cdc.gov/coronavirus/2019-ncov/if-you-are-sick/steps-when-sick.html; and

WHEREAS, persons without symptoms may be able to spread the COVID-19 virus. *See* https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/prevention.html; and

WHEREAS, fully vaccinated persons who become infected with the COVID-19 Delta variant can spread the virus to others. *See* https://www.cdc.gov/coronavirus/2019-ncov/vaccines/fully-vaccinated.html; and

WHEREAS, the City's public-meeting facilities are indoor facilities that do not ensure circulation of fresh / outdoor air, particularly during periods of cold and/or rainy weather, and were not designed to ensure that attendees can remain six (6) feet apart; and

WHEREAS, holding in-person meetings would encourage community members to come to City facilities to participate in local government, and some of them would be at high risk of getting very sick from COVID-19 and/or would live with someone who is at high risk; and

WHEREAS, in-person meetings would tempt community members who are experiencing COVID-19 symptoms to leave their homes in order to come to City facilities and participate in local government; and

WHEREAS, attendees would use ride-share services and/or public transit to travel to in-person meetings, thereby putting them in close and prolonged contact with additional people outside of their households; and

WHEREAS, on October 7, 2021, the Privacy Advisory Commission adopted a resolution determining that conducting in-person meetings would present imminent risks to attendees' health, and electing to continue conducting meetings using teleconferencing in accordance with California Government Code Section 54953(e), a provision of AB-361; now therefore be it:

RESOLVED: that the Privacy Advisory Commission finds and determines that the foregoing recitals are true and correct and hereby adopts and incorporates them into this resolution; and be it

FURTHER RESOLVED: that, based on these determinations and consistent with federal, state and local health guidance, the Privacy Advisory Commission renews its determination that conducting in-person meetings would pose imminent risks to the health of attendees; and be it

FURTHER RESOLVED: that the Privacy Advisory Commission firmly believes that the community's health and safety and the community's right to participate in local government, are both critically important, and is committed to balancing the two by continuing to use teleconferencing to conduct public meetings, in accordance with California Government Code Section 54953(e), a provision of AB-361; and be it

FURTHER RESOLVED: that the Privacy Advisory Commission will renew these (or similar) findings at least every thirty (30) days in accordance with California Government Code section 54953(e) until the state of emergency related to COVID-19 has been lifted, or the Privacy Advisory Commission finds that in-person meetings no longer pose imminent risks to the health of attendees, whichever occurs first.

CITY OF OAKLAND

Privacy Advisory Commission

November 4, 2021 5:00 PM
Teleconference
Meeting Minutes

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian Hofer, Chair, **District 4 Representative**: Lou Katz, **District 5 Representative**: Omar De La Cruz, **District 6 Representative**: Gina Tomlinson, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Henry Gage III, Vice Chair **Mayoral Representative**: Vacant*

1. Call to Order, determination of quorum

Members Present: Hofer, Gage, Oliver, Katz, Suleiman, De La Cruz, Tomlinson.

2. Adopt a Renewal Resolution regarding AB 361 establishing certain findings justifying the ongoing need for virtual meetings

The Resolution was adopted unanimously.

3. Review and approval of the draft October Special Meeting 1 and Meeting 2 Minutes

Both Special Meeting Minutes were approved unanimously with one correction: under the section on ALPR, Chair Hofer screen shared an analysis "of a single Bay Area jurisdiction," not the entire Bay Area.

4. Surveillance Equipment Ordinance – DOT – Dockless Mobility Data Sharing
    a. Review and take possible action on Annual Reports for 2020, 2021

Chair Hofer opened the item to acknowledge the early problems in Los Angeles regarding data retention that many were upset about—privacy avoicates and tech companies were aligned that LA's data retention policy was problematic. He pointed out that Oakland learned from LA's mistake and crafted a policy to avoid a similar problem here.

Kirby Olsen who oversees shared mobility programs for the Department of Transportation (OakDOT) presented the report. He noted that LA developed the "Mobility Data Standard" which is becoming the industry standard. Oakland does not need this data on its servers and limits the retention of it.

Kirby explained how the system works and displayed the maps the city uses to assess mobility vehicle distribution citywide which helps the City manage the program effectively. Because no user data is collected, the City can protect the privacy of the people using the vehicles.

Chairperson Hofer lauded the City's policy and Member Katz also noted that in this instance, the data is owned by the ride share companies, not the City. The fact that some data is shared with the City without impacting the privacy of the users is a great balance.

The PAC accepted the annual report unanimously.

5. Federal Task Force Transparency Ordinance – OPD – Drug Enforcement Agency MOU
   a. Review and take possible action on proposed memorandum of understanding

This item was pulled from the agenda.

6. Surveillance Equipment Ordinance – OPD – Automated License Plate Readers

Chair Hofer opened with his comments on the process and presented a spreadsheet of the findings the PAC adopted in May to display what progress had been made on these findings. On some, the situation improved, such as a lower retention period, but many others, in his opinion are unchanged. He stated that his position is unchanged, that he still supports a two-year moratorium on the use of ALPR by OPD.

Member Gage noted that ALPR technology is useful but that the data OPD provided did not justify its use due to the very low "hit rate" displayed in the reports. He also noted that the City Council may disagree, especially in this time of increased crime rates and public safety concerns. However, he went on to state the role of the PAC is to evaluate the civil liberties impact of the technology and how it is used and on that standard, he cannot support its current use.

Member Katz also noted the cost of the technology does not support its continued use. He also noted that mass surveillance typically hurts People of Color the most as well as people who challenge the power structure.

Member Suleiman drew a comparison between this technology and facial recognition technology in that the gathering of data through mass surveillance of this level needs to be held to a higher standard than other technologies and requires a higher level of trust in the department. She also believes the findings indicate the use should be discontinued.

Member De La Cruz reiterated what others said in his belief that the use does not come close to meeting the standard set in the law to allow for its continued use.

Captain Figueroa spoke on behalf of OPD and felt it was very unfortunate that there was no ad hoc committee to discuss more of the details of the policy as had been requested by OPD on several occasions but also noted he and the department respect the position of the PAC. He went on to note that the department believes it can fix the audit problem with a software upgrade that will cost approximately $15,000 which is a much lower cost than previously thought for a system upgrade. He is hopeful that this upgrade will provide the depth of data in the future that the PAC is looking for.

There were five public speakers on the item:

Alex Minus spoke in favor of ALPR technology and said he sees how it helps vulnerable communities. He himself is a shooting victim and believes the department needs this tool to do its work.

Jose Ruelas note he grew up in the Fruitvale and now lives in District 6. He sees a lot of crime in his neighborhood including a recent homicide on his block and believes OPD should be allowed to use this technology and that if people lived in the conditions he experiences, they would also support its use.

Oscar Yassin stated that he doesn't find it helpful for people to state what City Council District they live in as even district 6 has very affluent areas. He went on to state he agrees with the PAC position but believes the City Council will overrule the PAC anyway.

Sudip Ray noted he lives on Ney Avenue where there have been multiple shootings in the past several months and he believes one life saved is worth the cost of technology. He supports anything that will help OPD save more lives.

Assata Olugbala spoke about her personal experience, noting she lives in a safe community and hasn't personally been harassed and she believes surveillance is necessary to create safe spaces. She also noted that surveillance needs to be conducted properly.

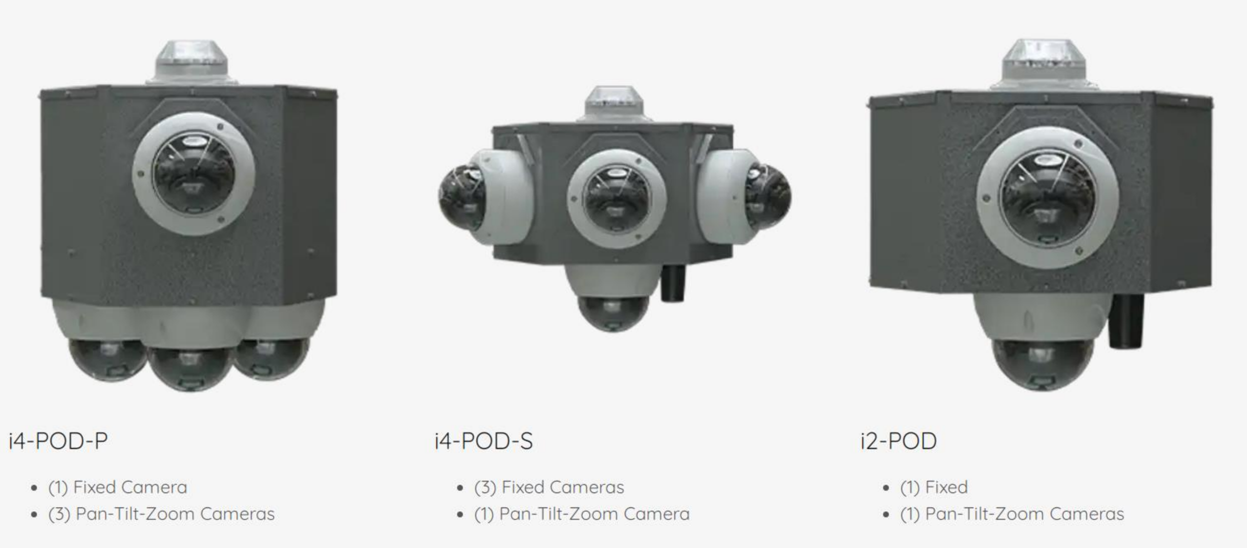
The PAC Chair restated his motion to uphold the original recommendation and the motion passed unanimously.

The meeting adjourned at 6:33pm.

City of Oakland

Public Works Department Surveillance Impact Report for Illegal Dumping Surveillance Cameras

A. **Description:**



The POD is an all-in-one, portable surveillance system. It comes in two basic models. The i4POD-P/ i4POD-S has four (4) cameras; the i2POD has two (2) cameras. Both models include a digital video recorder, a cellular router and a wifi transmitter – all housed in an easy to move and mount enclosure. The POD is plug and play; the City needs only to supply 110v power to activate system.

<u>i4POD-P and i4POD-S with 4 cameras</u>:

- One (1) or three (3) stationary cameras with 160-degree wide view.
- One (1) or three (3) pan/tilt/zoom cameras (PTZs) that offer 360 degrees view and zoom at 12x optical and 10x digital to enable flexibility to capture exactly what the user wants to see.

<u>i2POD with 2 cameras</u>:

- One (1) stationary camera with 160-degree wide view.
- One (1) PTZ camera that pans and tilts 360 degrees and zooms at 12x optical and 10x digital to enable flexibility to view exactly what the user wants to see.

<u>Additional “bullet” camera</u>: An additional bullet camera is used to enhance the ability to view license plates clearly. Bullet cameras do not store license plate information. There is no AI, no analytics, and no retention of license plate information in databases. All license plate information will be captured manually (visually) by the authorized user and sent to the City Attorney’s Office (OCA) to obtain DMV records.

<u>Digital video recorder (DVR)</u>: The POD DVR records video to a 2TB hard drive. It also streams encrypted video to the user using the POD desktop software, browser or

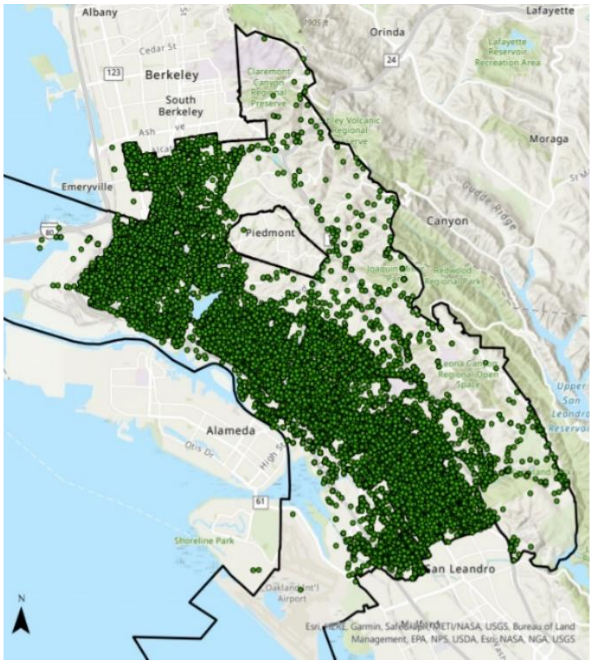
smartphone app. Video footage can be viewed live, searched, played back and downloaded via cellular or wifi connection.

Cellular router: Router uses internet service providers (ISPs) for connectivity, enabling user to access DVR and all other functions remotely.

Wifi transmitter: Wifi transmitter sends a wireless signal similar to a home or office router. It offers secondary access to a DVR and all of its functions if cellular signal is not available or if video is too large to transmit via cellular. User will drive up to a POD and connect an authorized laptop to the wifi signal, as one would at home or office.

IR Floodlight: Infrared lighting will be used to enhance video image capture in low/poor lighting locations. The IR Floodlight can illuminate an area like a flood light that only the camera can detect.

B. **Purpose:**


Albany
Berkeley
South Berkeley
Emeryville
Piedmont
Orinda
Lafayette
Moraga
Canyon
Alameda
Shoreline Park
San Leandro
N
Esri, HERE, Garmin, SafeGraph, METI/NASA, USGS, Bureau of Land Management, EPA, NPS, USDA, Esri, NASA, NGA, USGS

FY20-21 Illegal Dumping Work Orders Completed by KOCB

Illegal dumping is an epidemic in Oakland. The City is resolved to turn the tide on the widespread dumping by holding violators accountable. But as personnel necessary to deter dumping are limited, surveillance cameras offer the City a viable way to enhance/ support the investigative work performed by Oakland Public Works' (OPW's) four Environmental Enforcement Officers (EEOs). This Use Policy is for the operation of the POD – a surveillance system by Security Lines U.S.

The goal of installing POD units near chronic dumping hot spots is to capture video evidence that identifies dumpers or produces supporting information needed to build credible cases for prosecution. Staff believes there will be an immediate chilling effect on illegal dumping once the City prosecutes more cases using video evidence. Dumpers will have to re-evaluate their desire to dump against the higher risk of getting caught. Over time, surveillance cameras may serve as an ongoing, visual deterrent to potential dumpers after the surveillance program matures.

C. **Location:**

Cameras will be placed Citywide, in public rights of way nearest to chronic dumping "hot spots". Hot spots often contain dumping where there is insufficient evidence connecting the dumped piles to dumpers and therefore are ideal for surveillance cameras. Public rights of way include but are not limited to City assets such as street light poles, traffic signal poles, and other public assets like bus stop shelters (through coordination with AC Transit), and City-installed wooden posts. The City may also explore installing POD units on private properties through local business/private resident partnerships.

The POD's tamper-proof housing unit will be installed using simple mounting straps. Installations will be performed by Keep Oakland Clean & Beautiful (KOCB) staff. Preliminary plans are for the City to deploy POD systems in phases based on initial trial use, available funding, and Cityworks data tracking the effectiveness of surveillance cameras at chronic hot spots.

D. **Impact:**

OPW recognizes that all people have an inalienable right to privacy and are committed to protecting and safeguarding this right.

OPW does not seek to track movement of individuals. However, OPW understands that the public may be concerned that the surveillance, retention and analysis of video information over time could potentially be used to generate a detailed profile of an individual's movement or be abused for other inappropriate purposes.

Specifically, OPW recognizes the following public concerns:

- **Identity capture.** The public may be concerned that the cameras will capture personally identifiable information without notice or consent. And although POD surveillance cameras do not independently generate information that identifies vehicle occupants, license plate information can be used to determine the registered owner. In addition, vehicle occupants or immediate surroundings (including addresses) may be pictured. As a result, it is possible that individuals with access to this data could do additional research to identify the individual.

- **Misidentification.** The public may be concerned that individuals may be misidentified as the person driving a vehicle and is doing the dumping. This could lead to government actions against such individuals in error.

- **Activity monitoring.** The public may be concerned that the cameras' data will enable individuals' behaviors to be revealed to and/or monitored by OPW or other government agencies, their partners or affiliates, companies interested in targeted marketing, and/or the public. Such concerns may include basic information about when individuals are in certain locations, as well as concerns about what government or individuals may infer from this data (i.e. marital fidelity, religious observance, or political activity). Although video recordings and license plate numbers are gathered from public places, this could conflict with an individual's expectation of locational privacy.

E. **Mitigations:**

OPW will take multiple steps to mitigate privacy concerns:

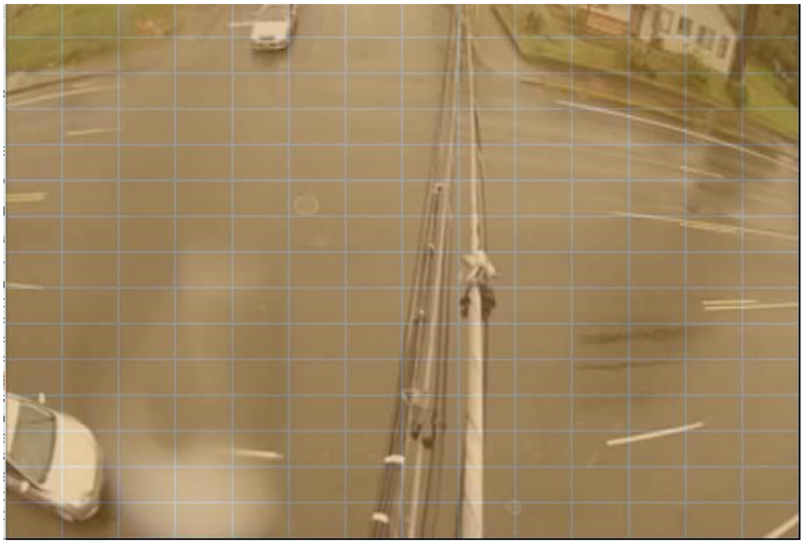
- OPW will use the POD surveillance system in accordance with the proposed *Illegal Dumping Surveillance Cameras Use Policy* (attached), as well as all applicable laws, policies and administrative instructions.

- OPW will not use or deploy the POD system in a discriminatory, viewpoint-based, or biased manner.

- **Surveillance systems will be deployed for the purpose of capturing illegal dumping activities only**. POD units will be installed in public rights of way (and potentially at local businesses and private properties through local business/ private resident partnerships) at or near known hot spots where chronic dumping occurs.

- The proposed POD system (i.e. cameras and software) does not contain analytics that track movement of individuals. To minimize the public being unnecessarily recorded, the POD's DVR may be set to record based on motion detection via pixel changes to specified areas of a camera's field of vision. The POD system can also mask or blackout sections of a video image that fall outside of the targeted dumping areas so that images such as houses, sidewalks, etc., can be made unviewable to all authorized users.

Example of how the City can select specific areas to activate motion-based recording.



- Bullet cameras do not use AI to analyze license plate information. All license plate information will be captured manually (visually) by the authorized user and referred to the City Attorney's Office (OCA) for DMV records. NOTE: Oakland Municipal Codes permit EEOs to cite both the dumper AND the owner of the vehicle used in a dumping incident. A robust appeal process is in place for individuals to appeal a citation if they feel they were cited in error.

- OPW will not purchase the additional equipment required to enable the POD's audio feature.

- OPW will limit admin/super user access to add/delete users and/or change user access to two (2) OPW Managers.

- Routine video recordings not downloaded will be purged automatically and permanently by the DVR every 14 days, when new video is saved over the oldest recordings.

- OPW will retain and use license plate information and video footage strictly for the enforcement of illegal dumping and will only forward footage containing illegal dumping activities to the OCA, assigned Hearing Officer, OPD and/or Alameda County's District Attorney's Office for prosecution.

- Data containing illegal dumping activities will be saved to a secure folder by authorized KOCB staff only. Downloaded video recordings and license plate information will be purged once filed claims, pending litigations, and/or criminal investigations conclude.

- OPW will conduct annual audits of license plate information and video footage to ensure compliance with destruction schedule and to verify that authorized users and administrators are following Use Policy.

- OPW shall report within 72 hours any Oakland Police Department (OPD) request for video recordings captured by POD units to the Chief Privacy Officer and Privacy Advisory Commission (PAC) Chair. OPD's request will describe the nature of the investigation for which the video data is being requested. This information will be reported to the PAC at its next regularly scheduled meeting.

- OPW will seek the Privacy Advisory Commission's review and recommendation prior to making changes to the POD's use.

F. **Data Types and Sources:**

- Image, video recordings
- License plate information as visible in video recordings
- Audit logs

G. **Data Security:**

Per *Public Works Department Surveillance Technology Use Policy for Illegal Dumping Surveillance Cameras*…

Data Access – There are three different levels of security to safeguard access to the video data.

1. Cellular router level: An authorized user's computer must be recognized by the cellular router ("Router") before s/he can gain access to the POD system. Personnel with "admin/super user" profiles will specify which computers' IP addresses the Router recognizes. A unique username/password is required to configure the Router.

2. Desktop software level: To interface with the POD system, proprietary POD software will be installed on an authorized user's computer. A unique username/password is required to access software. Different levels of POD access – view only, PTZ camera control, video search & download, and admin/super user access – may be assigned to different personnel by the admin/super user.

3. DVR level (for **optional** mobile phone application only): Each POD has its own DVR. To access a specific POD's recordings, a separate username/password is required to access the DVR associated with that POD. Like the desktop software, users may be added or removed and given different levels of access.

The City of Oakland has sole access to POD video data. Vendor Security Lines U.S. cannot access nor control POD units installed by their clients. The POD surveillance system does not connect to the Cloud. Furthermore, OPW will assign "occasional, as-needed" users with view only access, while select Environmental Enforcement Unit personnel will be granted view and PTZ control access, as well as clearance to search and download video footage. Finally, OPW will limit admin/super user access with the ability to add/delete users to two OPW personnel.

Individuals authorized to access and/or view surveillance camera information include:

Oakland Public Works –

- KOCB Operations Manager, who oversees the EEU, will be able to add/delete users and will be granted admin/super user access.

- OPW Bureau of Environment's Administrative Services Manager, who oversees the Illegal Dumping Surveillance Camera Use Policy, will be able to add/delete users and be given admin/super user access.

- Environmental Enforcement Unit (EEU) Supervisor and EEU Administrative Analyst, who will be tasked with checking cameras for illegal dumping activities and remote monitoring the POD units, will be given access to view video, control PTZ cameras, as well as search and download video evidence. EEU Supervisor and EEU Administrative Analyst will not have the ability to add or delete users.

- EEOs who investigate illegal dumping cases will be viewing and handling select video clips to gather and package evidence for the OCA. Security access to the POD system may be granted based on operational needs.

<u>Data Protection</u> – Since its introduction in 2009, the POD surveillance system has never been hacked. POD DVRs are Linux-based. Downloaded video is encrypted. Video recordings cannot be played using standard video players (e.g. Windows Media Player). Please refer to "*Data Access"* for the multi-level security measures required to access POD systems.

<u>Data Retention</u> – There are 2 ways video data are retained.

1. DVR hard drive: The POD DVR records video to the hard drive housed inside the POD unit. The hard drive automatically over-writes the oldest recordings.

Routine video recordings not downloaded will be purged automatically and permanently by the DVR every 14 days, when new video is saved on top of the oldest recordings.

2. Downloaded video: Video will only be downloaded when it contains adequate evidence of illegal dumping to warrant possible enforcement actions. An authorized user will download the video clips via the POD desktop software to a secure OPW folder. Downloaded recordings will be purged once filed claims, pending litigations, and/or criminal investigations conclude.

Public Access – Except where prohibited or limited by law, the public may access the City's video data through public records requests. However, prior to the release of any information to a surveillance-related public records request, staff will consult with the City Attorney's Office for review and guidance.

Third Party Data Sharing – There is no third-party data sharing with the POD surveillance system. The vendor cannot access the City's video data through the POD software. Computers with IP addresses entered by the City's admin/super user are the only computers permitted to access the PODs. (See "*Data Access"*) The POD Surveillance System does not connect to the Cloud.

Other City departments or non-City entities that may view or use POD video recordings are:

City Attorney's Office (OCA) –

- ➢ Assigned City Attorney in OCA's Litigation Unit will view select video clips 1) to ascertain the viability of the video evidence, and 2) to work up a case to initiate legal actions to prosecute the dumper for violations of the Oakland Municipal Code. Security access to the POD system is not required.

Administrative Hearing Officer –

- ➢ Assigned Administrative Hearing Officer may view select video clips in the course of adjudicating illegal dumping cases. Security access to the POD system is not required.

Oakland Police Department (OPD) / Alameda County District Attorney's (DA's) Office –

- ➢ In the event POD cameras capture illegal dumping of the scale and/or nature that warrant criminal investigations, EEU staff may share select video clips with OPD and/or the DA's Office for further illegal dumping investigatory and enforcement actions. Security access to the POD system is not required.

H. Fiscal Cost:

The i2POD, i4POD-S, and i4POD-P are priced at $5495, $7195, and $7995 respectively. Installation will be performed by KOCB staff but can also be installed by the vendor for a one-time fee. There are no mandatory annual maintenance service fees or initial per camera licensing fees. Ongoing cost consists of monthly cellular service.

The monitoring of the POD system and the reviewing/searching/downloading of video footage containing potentially enforceable illegal dumping activities will be performed by the EEU's Analyst. Time required to perform job duties associated with the new surveillance cameras will likely necessitate one additional administrative personnel to assume portions of the Analyst's current job duties.

Funding to purchase the trial POD units is available in the FY21-23 Approved Budget in ORGs 30674/30676.

I. Third Party Dependence:

Cellular service provided by the City's ISP(s). The POD Surveillance System does not connect to the Cloud.

J. Alternatives:

Status Quo - Do not deploy surveillance cameras. There will not be any financial outlay for surveillance cameras. However, illegal dumping abatement costs (over $5.6M in annual expenditure for FY20-21) will likely continue to rise precipitously if the City continues operation as is. The City will need to answer to the constituents demanding the City take decisive action against dumpers. The City will continue to struggle with addressing dumping at chronic hot spots.

Sting Operations with OPD - Request assistance from OPD to conduct sting operations at chronic hot spots to catch dumpers in the act. This is not a viable solution because: 1) it is cost prohibitive; 2) OPW has been advised on multiple occasions OPD does not have the resources to assist with illegal dumping enforcement due to higher priority crimes; 3) the Mayor and CAO may likely not support allocating sworn officers to illegal dumping enforcement.

Hire More EEOs - Bring on more EEOs to patrol hot spots and to catch dumpers. Funding to hire three additional EEOs is in place for FY22-23. Nevertheless, this is not a viable long term solution because: 1) it will be cost prohibitive to hire enough EEOs to provide adequate coverage of areas prone to chronic dumping; 2) more EEOs does not necessarily translate to greater success in catching dumpers if there is insufficient evidence to prosecute. Without supporting evidence, the only way an EEOs can catch a dumping violator is to witness the individual in the act of dumping.

K. **Track Record:**

San Leandro, Sacramento, Fremont, Alameda, Livermore, and Milpitas are just a few of the regional municipalities using the POD surveillance system. In October 2021, OPW staff solicited product reviews from the City of Alameda and the City of Livermore. Both cities gave full endorsements for the product. Key features of the POD system that garnered positive reviews were:

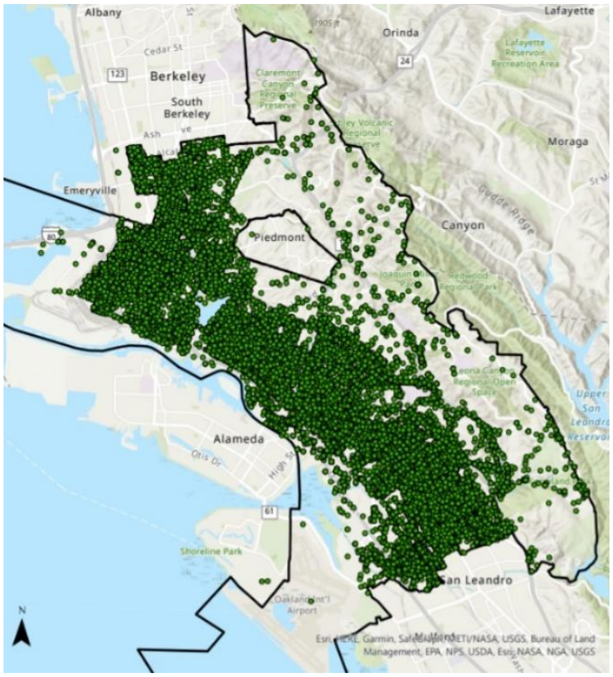
- Tamper-proof housing unit: weather-tested, near-indestructible casing
- Easy set-up: system only requires 110v power, mounting bracket, and mounting straps to install
- Mobile: easy to move unit to other locations
- Reliability: minimal downtime with stable cellular service
- Minimal maintenance: simple design makes for minimal maintenance
- Simple to use
- Clean, crisp video images

Neither Security Line U.S. nor the POD system has experienced any data breach since its introduction in 2009.

City of Oakland

Public Works Department Surveillance Technology Use Policy for Illegal Dumping Surveillance Cameras

A. Purpose



FY20-21 Illegal Dumping Work Orders Completed by KOCB

Illegal dumping is an epidemic in Oakland. The City is resolved to turn the tide on the widespread dumping by holding violators accountable. But as personnel necessary to deter dumping are limited, surveillance cameras offer the City a viable way to enhance/ support the investigative work performed by Oakland Public Works' (OPW's) four Environmental Enforcement Officers (EEOs). This Use Policy is for the operation of the POD – a surveillance system by Security Lines U.S.

The goal of installing POD units near chronic dumping hot spots is to capture video evidence that identifies dumpers or produces supporting information needed to build credible cases for prosecution. Staff believes there will be an immediate chilling effect on illegal dumping once the City prosecutes more cases using video evidence. Dumpers will have to re-evaluate their desire to dump against the higher risk of getting caught. Over time, surveillance cameras may serve as an ongoing, visual deterrent to potential dumpers after the surveillance program matures.

B. Authorized Use

Authorized use of the POD surveillance system:

- surveilling illegal dumping activity in the City of Oakland

Only staff with a need to know and a right to know will have access to recordings captured by the POD system. See sections **D. Data Access,** and **H. Third Party Data Sharing**, for a list of individuals who will be authorized to access and/or view surveillance data.

C. Data Collection

Data collection occurs inside a POD housing unit near chronic illegal dumping hot spots. Video captured from the cameras are recorded directly to the digital video recorder's (DVR's) hard drive (2 TB SATA). DVRs do not possess artificial intelligence (AI) or analytics such as facial recognition. The POD surveillance system does not connect to the Cloud.

D. Data Access

There are three different levels of security to safeguard access to the video data.

1. Cellular router level: An authorized user's computer must be recognized by the cellular router ("Router") before s/he can gain access to the POD system. Personnel with "admin/super user" profiles will specify which computers' IP addresses the Router recognizes. A unique username/password is required to configure the Router.

2. Desktop software level: To interface with the POD system, proprietary POD software will be installed on an authorized user's computer. A unique username/password is required to access software. Different levels of POD access – view only, PTZ camera control, video search & download, and admin/super user access – may be assigned to different personnel by the admin/super user.

3. DVR level (for **optional** mobile phone application only): Each POD has its own DVR. To access a specific POD's recordings, a separate username/password is required to access the DVR associated with that POD. Like the desktop software, users may be added or removed and given different levels of access.

The City of Oakland has sole access to POD video data. Vendor Security Lines U.S. cannot access nor control POD units installed by their clients. The POD surveillance system does not connect to the Cloud. Furthermore, OPW will assign "occasional, as-needed" users with view only access, while select Environmental Enforcement Unit personnel will be granted view and PTZ control access, as well as clearance to search and download video footage. Finally, OPW will limit admin/super user access with the ability to add/delete users to two OPW personnel.

Individuals authorized to access and/or view surveillance camera information include:

Oakland Public Works –

- KOCB Operations Manager, who oversees the EEU, will be able to add/delete users and will be granted admin/super user access.

- OPW Bureau of Environment's Administrative Services Manager, who oversees the Illegal Dumping Surveillance Camera Use Policy, will be able to add/delete users and be given admin/super user access.

- Environmental Enforcement Unit (EEU) Supervisor and EEU Administrative Analyst, who will be tasked with checking cameras for illegal dumping activities and remote monitoring the POD units, will be given access to view video, control PTZ cameras, as well as search and download video evidence. EEU Supervisor and EEU Administrative Analyst will not have the ability to add or delete users.
- EEOs who investigate illegal dumping cases will be viewing and handling select video clips to gather and package evidence for the OCA. Security access to the POD system may be granted based on operational needs.

E. Data Protection

Since its introduction in 2009, the POD surveillance system has never been hacked. POD DVRs are Linux-based. Downloaded video is encrypted. Video recordings cannot be played using standard video players (e.g. Windows Media Player). Please refer to section **D. Data Access** for the multi-level security measures required to access POD systems.

F. Data Retention

There are 2 ways video data are retained.

1. DVR hard drive: The POD DVR records video to the hard drive housed inside the POD unit. The hard drive automatically over-writes the oldest recordings. Routine video recordings not downloaded will be purged automatically and permanently by the DVR every 14 days, when new video is saved on top of the oldest recordings.
2. Downloaded video: Video will only be downloaded when it contains adequate evidence of illegal dumping to warrant possible enforcement actions. An authorized user will download the video clips via the POD desktop software to a secure OPW folder. Downloaded recordings will be purged once filed claims, pending litigation, and/or criminal investigations and prosecutions conclude.

G. Public Access

Except where prohibited or limited by law, the public may access the City’s video data through public records requests. However, prior to the release of any information to a surveillance-related public records request, staff will consult with the City Attorney’s Office for review and guidance.

H. Third Party Data Sharing

There is no third-party data sharing with the POD surveillance system. The vendor cannot access the City's video data through the POD software. Computers with IP addresses entered by the City's admin/super user are the only computers permitted to access the PODs. (See section **D. Data Access**) The POD surveillance system does not connect to the Cloud.

Other City departments or non-City entities that may view or use POD video recordings are:

City Attorney's Office (OCA) –

- ➢ Assigned City Attorney staff in OCA's Litigation Division will view select video clips 1) to ascertain the viability of the video evidence, and 2) to work up a case to initiate legal actions to prosecute the dumper for violations of the Oakland Municipal Code. Security access to the POD system is not required.

Administrative Hearing Officer –

- ➢ Assigned Administrative Hearing Officer may view select video clips in the course of adjudicating illegal dumping cases via the City's administrative hearings (due process hearings for violators that appeal the City's determinations on violations). Security access to the POD system is not required.

Oakland Police Department (OPD)/ Alameda County District Attorney's (DA's) Office –

- ➢ In the event POD cameras capture illegal dumping of the scale and/or nature that warrant criminal investigations, EEU staff may share select video clips with OPD and/or the DA's Office for further illegal dumping investigatory and enforcement actions. Security access to the POD system is not required.

I. Training

Training is available in video tutorials and written formats on vendor Security Lines U.S.'s website in a members-only area. One on one remote training is available.
The Administrative Services Manager in OPW's Bureau of Environment shall conduct training with authorized POD users. Training will include reading this Use Policy and reviewing operational procedures required to adhere to the Policy.

J. Auditing and Oversight

The Administrative Services Manager in OPW's Bureau of Environment shall conduct annual assessments to ensure authorized users comply with the Use Policy.

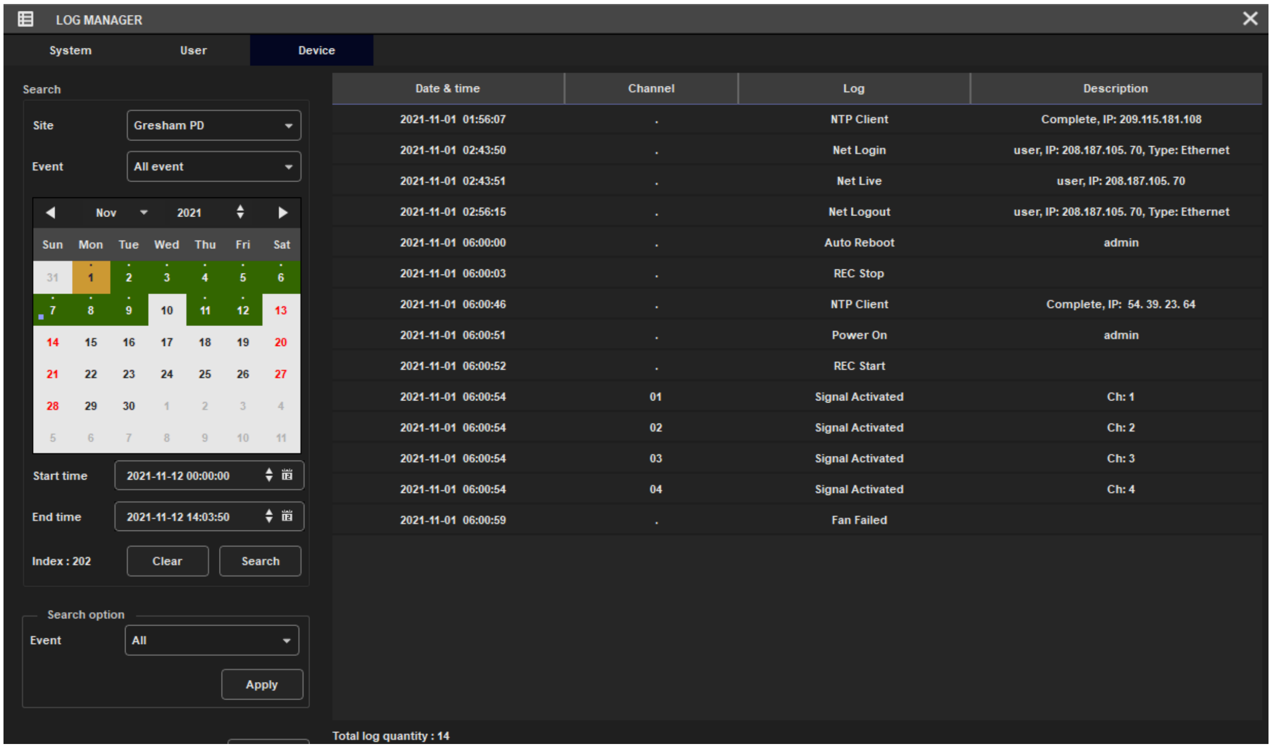
All POD user and device activity are logged. Designated admin/super users can access and view audit logs at the camera level. The audit log tracks system access and ties each action to a user for events such as:

- User Log-ins/ Log-outs by IP address
- User Management (add, edit, delete users; settings imported/exported)

The audit log also tracks device specific events such as:

- Recordings stopped and started
- Reboots
- Power On
- Time syncs

Example of audit log.



Site: Gresham PD

Event: All event

Nov			2021			
Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4
5	6	7	8	9	10	11

Start time: 2021-11-12 00:00:00

End time: 2021-11-12 14:03:50

Index : 202

Search option

Event: All

Date & time	Channel	Log	Description
2021-11-01 01:56:07	.	NTP Client	Complete, IP: 209.115.181.108
2021-11-01 02:43:50	.	Net Login	user, IP: 208.187.105. 70, Type: Ethernet
2021-11-01 02:43:51	.	Net Live	user, IP: 208.187.105. 70
2021-11-01 02:56:15	.	Net Logout	user, IP: 208.187.105. 70, Type: Ethernet
2021-11-01 06:00:00	.	Auto Reboot	admin
2021-11-01 06:00:03	.	REC Stop	
2021-11-01 06:00:46	.	NTP Client	Complete, IP: 54. 39. 23. 64
2021-11-01 06:00:51	.	Power On	admin
2021-11-01 06:00:52	.	REC Start	
2021-11-01 06:00:54	01	Signal Activated	Ch: 1
2021-11-01 06:00:54	02	Signal Activated	Ch: 2
2021-11-01 06:00:54	03	Signal Activated	Ch: 3
2021-11-01 06:00:54	04	Signal Activated	Ch: 4
2021-11-01 06:00:59	.	Fan Failed	

Total log quantity : 14

K. Maintenance

Security Lines U.S. offers but does not require a maintenance contract. The POD's simple, rugged design requires minimal maintenance. Vendor and existing client testimonials suggest that maintenance, when required, constituted the occasional replacement of a hard drive or camera cover, which most client organizations service themselves.