32

Office of the City Manager

ACTION CALENDAR
November 3, 2022

To: Honorable Mayor and Members of the City Council

From: Dee Williams-Ridley, City Manager

Submitted by: Jennifer Louis, Interim Chief of Police
Liam Garland, Director of Public Works
LaTanya Bellow, Deputy City Manager

Subject: Resolution Accepting the Annual Surveillance Technology Reports for Automatic License Plate Readers, GPS Trackers, Body Worn Cameras, Unmanned Aerial Vehicles (UAV's) and the Street Level Imagery Project Pursuant to Chapter 2.99 of the Berkeley Municipal Code

RECOMMENDATION

Adopt a Resolution Accepting the Surveillance Technology Report for Automatic License Plate Readers, GPS Trackers, Body Worn Cameras, Unmanned Aerial Vehicles (UAV's) and the Street Level Imagery Project Pursuant to Chapter 2.99 of the Berkeley Municipal Code.

FISCAL IMPACTS OF RECOMMENDATION

There are no fiscal impacts associated with adopting the attached resolution.

CURRENT SITUATION AND ITS EFFECTS

On March 27, 2018, the City Council adopted Ordinance 7,592-N.S., adding Chapter 2.99 to the Berkeley Municipal Code, which is also known as the Surveillance Technology Use and Community Safety Ordinance ("Ordinance"). The purpose of the Ordinance is to provide transparency surrounding the use of surveillance technology, as defined by Section 2.99.020 in the Ordinance, and to ensure that decisions surrounding the acquisition and use of surveillance technology consider the impacts that such technology may have on civil rights and civil liberties. Further, the Ordinance requires that the City evaluate all costs associated with the acquisition of surveillance technology and regularly report on their use.

The Ordinance imposes various reporting requirements on the City Manager and staff. The purpose of this staff report and attached resolution is to satisfy the annual reporting requirement as outlined in Section 2.99.070.

One of the reporting categories of the surveillance technology use is whether complaints have been received by the community about the various technologies. To

date Berkeley Police Department Internal Affairs Bureau (IAB) has not received any external personnel complaints surrounding these technologies. External complaints from community members can be made in writing, via email, in person or via telephone. Complaints can be received with direct communication to Internal Affairs from the complainant and/or be received by any member of the Department and then forwarded through the chain of command. If a community member initiates a complaint against a subject employee and during the investigation it is determined the subject employee violated policy regarding the misuse of technology, an additional complaint is initiated by the Chief of Police.

Community members also have the right to initiate complaints against employees of BPD by reporting directly to the Police Accountability Board (PAB). The Director of Police Accountability notifies the Chief of Police when an investigation into a complaint is initiated by the PAB, which would prompt a parallel IAB investigation.

Attached to this staff report are Surveillance Technology Reports for Automatic License Plater Readers, GPS Trackers, Body Worn Cameras, and the Street Level Imagery Project. Additionally, this year the Berkeley Police Department had three exigent uses pursuant to BMC 2.99.040 in which the City Manager authorized the Police Department to temporarily use an Unmanned Aerial Vehicle, commonly referred to as a drone, for critical incidents. These incidents were reported by the City Manager to Council pursuant to 2.99.040(2) and are included in this annual report pursuant to BMC 2.99.040(3). At this time the Berkeley Police Department does not intend to acquire this technology but is actively consulting with the City Attorney's Office regarding developing a Use Policy.

BACKGROUND

On March 27, 2018, the City Council adopted Ordinance 7,592-N.S., adding Chapter 2.99 to the Berkeley Municipal Code, which is also known as the Surveillance Technology Use and Community Safety Ordinance. Section 2.99.070 of the Ordinance requires that the City Manager must submit to the City Council a Surveillance Technology Report as defined by Section 2.99.020(2) of the Ordinance at the first regular City Council meeting in November.

For each of the four technologies, the Surveillance Technology Reports were prepared to satisfy the specific, section-by-section requirements of the Ordinance, and are attached to this report. Also attached is the Surveillance Technology Report for the temporary uses of an Unmanned Aerial Vehicle commonly referred to as a drone pursuant to BMC 2.99.040.

The Surveillance Technology Use Policy for ALPR technology was unanimously adopted at Council on September 13th, 2022 under Resolution 70,524_N.S..

ENVIRONMENTAL SUSTAINABILITY AND CLIMATE IMPACTS
There are no identifiable environmental effects or opportunities associated with the content of this report.

RATIONALE FOR RECOMMENDATION
City Council is being requested to adopt the attached resolution for the City to be in compliance with the Ordinance.

ALTERNATIVE ACTIONS CONSIDERED
City Council could decide not to adopt the resolution.

CONTACT PERSON
Jennifer Louis, Interim Chief of Police, (510) 981-5700
LaTanya Bellow, Deputy City Manager, (510) 981-7012

ATTACHMENTS
1. Resolution

2. Body Worn Cameras
   a) Surveillance Technology Report: Body Worn Cameras
   b) Retention Schedule

3. Global Positioning System (GPS) Tracking Devices
   Surveillance Technology Report

4. Automated License Plate Readers
   Surveillance Technology Report

5. Street Level Imagery Project
   Surveillance Technology Report

6. Unmanned Aerial Vehicle (UAV's)
   Surveillance Technology Report

RESOLUTION NO. XX,XXX-N.S.

ACCEPTING THE SURVEILLANCE TECHNOLOGY REPORT FOR AUTOMATIC LICENSE PLATE READERS, GPS TRACKERS, BODY WORN CAMERAS, UNMANNED AERIAL VEHICLES (UAV'S) AND THE STREET LEVEL IMAGERY PROJECT

WHEREAS, on March 27, 2018, the City Council adopted Ordinance 7,592-N.S., which is known as the Surveillance Technology Use and Community Safety Ordinance ("Ordinance"); and

WHEREAS, Section 2.99.070 of the Ordinance requires that the City Manager must submit to the City Council a Surveillance Technology Report as defined by Section 2.99.020(2) of the Ordinance at the first regular City Council meeting in November; and

WHEREAS, the Surveillance Technology Reports satisfy the requirements of the Ordinance.

NOW THEREFORE, BE IT RESOLVED by the Council of the City of Berkeley that the Council hereby accepts the Surveillance Technology Reports for Automatic License Plate Readers, GPS Trackers, Body Worn Cameras, Unmanned Aerial Vehicles (UAV's) and the Street Level Imagery Project.

ORDINANCE NO. 7,592–N.S.

ADDING CHAPTER 2.99 TO THE BERKELEY MUNICIPAL CODE, ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY

BE IT ORDAINED by the Council of the City of Berkeley as follows:

Section 1. Title
This ordinance shall be known as the Surveillance Technology Use and Community Safety Ordinance.

Section 2. That Chapter 2.99 is hereby added to the Berkeley Municipal Code to read as follows:

Chapter 2.99

Acquisition and Use of Surveillance Technology

2.99.010 Purposes
2.99.020 Definitions
2.99.030 City Council Approval Requirement
2.99.040 Temporary Acquisition and Use of Surveillance Equipment
2.99.050 Compliance for Existing Surveillance Technology
2.99.060 Determination by City Council that Benefits Outweigh Costs and Concerns
2.99.070 Oversight Following City Council Approval
2.99.080 Public Access to Surveillance Technology Contracts
2.99.090 Enforcement
2.99.100 Whistleblower Protections
2.99.110 Severability

2.99.010 Purposes
A. Through the enactment of this Chapter, the City seeks to establish a thoughtful process regarding the procurement and use of Surveillance Technology that carefully balances the City's interest in protecting public safety with its interest in protecting the privacy and civil rights of its community members.
B. Transparency is essential when the City is considering procurement and use of Surveillance Technology.
C. Although such technology may be beneficial to public order and safety, it has the potential to put both privacy and civil liberties at risk.
D. Decisions relating to Surveillance Technology should occur with strong consideration of the impact such technologies may have on civil rights and civil liberties, as with all rights guaranteed by the California and United States Constitutions.
E. Surveillance Technology may involve immediate, as well as ongoing, financial costs. Before the City acquires any Surveillance Technology, it must evaluate all costs associated with the procurement, installation, use and maintenance of the technology.

F. Decisions regarding whether and how Surveillance Technologies should be funded, acquired, or used should be governed by the City Council as the elected representatives of the City.
G. In addition to applicable local, state, and federal law, legally enforceable safeguards, including robust transparency, oversight, and accountability measures, are important in the protection of civil rights and civil liberties.
H. Data reporting measures will enable the City Council and public to confirm that mandated civil rights and civil liberties safeguards have been strictly observed.

2.99.020 Definitions
The following definitions apply to this Chapter:

1. "Surveillance Technology" means an electronic device, system utilizing an electronic device, or similar technological tool used, designed, or primarily intended to collect 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 covered Surveillance Technology include, but are not limited to: cell site simulators (Stingrays); automatic license plate readers; body worn cameras; gunshot detectors (ShotSpotter); facial recognition software; thermal imaging systems, except as allowed under Section 2(d); social media analytics software; gait analysis software; and video cameras that record audio or video and can remotely transmit or can be remotely accessed.

"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 2 (above):

a. Routine office hardware, such as televisions, computers, and printers, that is in widespread public use and will not be used for any surveillance functions;
b. Handheld Parking Citation Devices, that do not automatically read license plates;
c. Manually-operated, portable digital cameras, audio recorders, and video recorders that are not to be used remotely and whose functionality is limited to manually capturing, viewing, editing and downloading video and/or audio recordings, but not including body worn cameras;
d. Devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles or thermal imaging cameras used for fire operations, search and rescue operations and missing person searches, and equipment used in active searches for wanted suspects;
e. annually-operated technological devices that are not designed and will not be used to surreptitiously collect surveillance data, such as two-way radios,
email systems and city-issued cell phones;
f. Municipal agency databases;
g. Medical equipment used to diagnose, treat, or prevent disease or injury, including electrocardiogram machines;
h. Cybersecurity capabilities, technologies and systems used by the City of Berkeley Department of Information Technology to predict, monitor for, prevent, and protect

technology infrastructure and systems owned and operated by the City of Berkeley from potential cybersecurity events and cyber-forensic based investigations and prosecutions of illegal computer based activity;
i. Stationary security cameras affixed to City property or facilities.

2. "Surveillance Technology Report" means an annual written report by the City Manager covering all of the City of Berkeley's Surveillance Technologies that includes all of the following information with regard to each type of Surveillance Technology:

a. Description: A description of all non-privileged and non-confidential information about use of the Surveillance Technology, including but not limited to the quantity of data gathered and sharing of data, if any, with outside entities. If sharing has occurred, the report shall include general, non-privileged and non- confidential information about recipient entities, including the names of the entities and purposes for such sharing;
b. Geographic Deployment: Where applicable, non-privileged and non- confidential information about where the surveillance technology was deployed geographically;
c. Complaints: A summary of each complaint, if any, received by the City about the Surveillance Technology;
d. Audits and Violations: The results of any non-privileged internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response;
e. Data Breaches: Non-privileged and non-confidential 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;
f. Effectiveness: Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes;
g. Costs: Total annual costs for the Surveillance Technology, including personnel and other ongoing costs.

3. "Surveillance Acquisition Report" means a publicly-released written report produced prior to acquisition or to proposed permanent use after use in Exigent Circumstances pursuant to Section 2.99.040 (2), of a type of Surveillance Technology that includes the following:

a. Description: Information describing the Surveillance Technology and how it works, including product descriptions from manufacturers;
b. Purpose: Information on the proposed purposes(s) for the Surveillance Technology;
c. Location: The general location(s) it may be deployed and reasons for deployment;
d. Impact: An assessment identifying potential impacts on civil liberties and civil rights including but not limited to potential disparate or adverse impacts on any communities or groups;
e. Mitigation: Information regarding technical and procedural measures that can be implemented to appropriately safeguard the public from any impacts identified in

subsection (d);
f. Data Types and Sources: A list of the sources of data proposed to be collected, analyzed, or processed by the Surveillance Technology, including “open source” data;
g. Data Security: Information about the steps that can be taken to ensure adequate security measures to safeguard the data collected or generated from unauthorized access or disclosure;
h. Fiscal Cost: The fiscal costs for the Surveillance Technology, including initial purchase, personnel and other ongoing costs, including to the extent practicable costs associated with compliance with this and other reporting and oversight requirements, as well as any current or potential sources of funding;
i. Third Party Dependence and Access: 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, and whether a third-party may have access to such data or may have the right to sell or otherwise share the data in aggregated, disaggregated, raw or any other formats;
j. Alternatives: A summary and general assessment of potentially viable alternative methods (whether involving the use of a new technology or not), if any, considered before deciding to propose acquiring the Surveillance Technology. , ; and,
k. Experience of Other Entities: To the extent such information is available, a summary of the experience of comparable government entities with the proposed technology, including any unanticipated financial or community costs and benefits, experienced by such other entities.

4. "Surveillance Use Policy" means a publicly-released and legally-enforceable policy for use of each type of the Surveillance Technology that shall reflect the Surveillance Acquisition Report produced for that Surveillance Technology and 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 uses that are authorized, the rules and processes required prior to such use, and the uses that are prohibited;
c. Data Collection: Information collection that is allowed and prohibited. Where applicable, list any data sources the technology will rely upon, including “open source” data;
d. Data Access: A general description of the title and position of the employees and entities authorized to access or use the collected information, and the rules and processes required prior to access or use of the information, and a description of any and all of the vendor’s rights to access and use, sell or otherwise share information for any purpose;
e. Data Protection: A general description of the safeguards that protect information from unauthorized access, including encryption and access control mechanisms, and safeguards that exist to protect data at the vendor level;
f. Civil Liberties and Rights Protection: A general description of the safeguards that protect against the use of the Surveillance Technology and any data resulting from

its use in a way that violates or infringes on civil rights and liberties, including but not limited to potential disparate or adverse impacts on any communities or groups;
g. 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 such period;
h. Public Access: How collected information may be accessed or used by members of the public;
i. Third Party Data Sharing: If and how other City 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;
j. Training: Training required for any employee authorized to use the Surveillance Technology or to access information collected;
k. Auditing and Oversight: Mechanisms to ensure that the Surveillance Use Policy is followed, technical measures to monitor for misuse, and the legally enforceable sanctions for intentional violations of the policy; and
l. Maintenance: The mechanisms and procedures to ensure maintenance of the security and integrity of the Surveillance Technology and collected information.

5. “Exigent Circumstances” means the City Manager’s good faith belief that an emergency involving imminent danger of death or serious physical injury to any person, or imminent danger of significant property damage, requires use of the Surveillance Technology or the information it provides.

2.99.030 City Council Approval Requirement
1. The City Manager must obtain City Council approval, except in Exigent Circumstances, by placing an item on the Action Calendar at a duly noticed meeting of the City Council prior to any of the following:

a. Seeking, soliciting, or accepting grant funds for the purchase of, or in-kind or other donations of, Surveillance Technology;
b. Acquiring new Surveillance Technology, including but not limited to procuring such technology without the exchange of monies or consideration;
c. Using new Surveillance Technology, or using Surveillance Technology previously approved by the City Council for a purpose, or in a manner not previously approved by the City Council; or
d. Entering into an agreement with a non-City entity to acquire, share or otherwise use Surveillance Technology or the information it provides, or expanding a vendor’s permission to share or otherwise use Surveillance Technology or the information it provides.

2. The City Manager must present a Surveillance Use Policy for each Surveillance Technology to the Police Review Commission, prior to adoption by the City Council. The Police Review Commission shall also be provided with the corresponding Surveillance Acquisition Report that had been presented to council for that Surveillance Technology.

No later than 30 days after receiving a Surveillance Use Policy for review, the Police Review Commission must vote to recommend approval of the policy, object to the proposal, recommend modifications, or take no action. Neither opposition to approval of such a policy, nor failure by the Police Review Commission to act shall prohibit the City Manager from proceeding with its own review and potential adoption.

3. The City Manager must submit for review a Surveillance Acquisition Report and obtain City Council approval of a Surveillance Use Policy prior to engaging in any of the activities described in subsection (1) (a)-(d).

2.99.040 Temporary Acquisition and Use of Surveillance Equipment
Notwithstanding the provisions of this Chapter, the City Manager may borrow, acquire and/or temporarily use Surveillance Technology in Exigent Circumstances without following the requirements in Sections 2.99.030 and 2.99.040. However, if the City Manager borrows, acquires or temporarily uses Surveillance Technology in Exigent Circumstances he or she must take all of the following actions:

1. Provide written notice of that acquisition or use to the City Council within 30 days following the commencement of such Exigent Circumstance, unless such information is confidential or privileged;
2. If it is anticipated that the use will continue beyond the Exigent Circumstance, submit a proposed Surveillance Acquisition Report and Surveillance Use Policy, as applicable, to the City Council within 90 days following the borrowing, acquisition or temporary use, and receive approval, as applicable, from the City Council pursuant to Sections 2.99.030 and 2.99.040; and
3. Include the Surveillance Technology in the City Manager's next annual Surveillance Technology Report.

2.99.050 Compliance for Existing Surveillance Technology
The City Manager shall submit to the Action Calendar for the first City Council meeting in November of 2018, a Surveillance Acquisition Report and a proposed Surveillance Use Policy for each Surveillance Technology possessed or used prior to the effective date of this ordinance.

2.99.060 Determination by City Council that Benefits Outweigh Costs and Concerns
The City Council shall only approve any action described in Section 2.99.030, 2.99.040, or Section 2.99.050 of this Chapter after making a determination that the benefits to the community of the Surveillance Technology, used according to its Surveillance Use Policy, outweigh the costs; that the proposal will appropriately safeguard civil liberties and civil rights to the maximum extent possible while serving its intended purposes; and that, in the City Council's judgment, no feasible alternative with similar utility and a lesser impact on civil rights or civil liberties could be implemented.

2.99.070 Oversight Following City Council Approval
The City Manager must submit to the Council Action Calendar a written Surveillance

Technology Report, covering all of the City's Surveillance Technologies, annually at the first regular Council meeting in November. After review of the Surveillance Technology Report, Council may make modifications to Surveillance Use Policies.

2.99.080 Public Access to Surveillance Technology Contracts
To the extent permitted by law, the City shall continue to make available to the public all of its surveillance-related contracts, including related non-disclosure agreements, if any.

2.99.090 Enforcement
This Chapter does not confer any rights upon any person or entity other than the City Council to cancel or suspend a contract for a Surveillance Technology. The Chapter does not provide a private right of action upon any person or entity to seek injunctive relief against the City or any employee unless that person or entity has first provided written notice to the City Manager by serving the City Clerk, regarding the specific alleged violations of this Chapter. If a specific alleged violation is not remedied within 90 days of that written notice, a person or entity may seek injunctive relief in a court of competent jurisdiction. If the alleged violation is substantiated and subsequently cured, a notice shall be posted in a conspicuous manner on the City's website that describes, to the extent permissible by law, the corrective measures taken to address the violation. If it is shown that the violation is the result of arbitrary or capricious action by the City or an employee or agent thereof in his or her official capacity, the prevailing complainant in an action for relief may collect from the City reasonable attorney's fees in an amount not to exceed $15,000 if he or she is personally obligated to pay such fees.

2.99.100 Whistleblower Protections
All provisions of Berkeley's Protection of Whistleblowers Workplace Policy, as promulgated by the City Manager on November 2, 2016 and including any updates or replacements thereto, shall apply.

2.99.110 Severability
If any word, phrase, sentence, part, section, subsection, or other portion of this Chapter, or any application thereof to any person or circumstance is declared void, unconstitutional, or invalid for any reason, then such word, phrase, sentence, part, section, subsection, or other portion, or the prescribed application thereof, shall be severable, and the remaining provisions of this Chapter, and all applications thereof, not having been declared void, unconstitutional or invalid, shall remain in full force and effect. The City Council hereby declares that it would have passed this title, and each section, subsection, sentence, clause and phrase of this Chapter, irrespective of the fact that any one or more sections, subsections, sentences, clauses or phrases is declared invalid or unconstitutional.

Section 3. Copies of this Ordinance shall be posted for two days prior to adoption in the display case located near the walkway in front of Council Chambers, 2134 Martin Luther King Jr. Way. Within 15 days of adoption, copies of this Ordinance shall be filed at each branch of the Berkeley Public Library and the title shall be published in a newspaper of general circulation.

At a regular meeting of the Council of the City of Berkeley held on March 13, 2018, this Ordinance was passed to print and ordered published by posting by the following vote:

Ayes: Bartlett, Davila, Droste, Hahn, Harrison, Maio, Wengraf, Worthington and Arreguin.

Noes: None.

Absent: None.

Surveillance Technology Report: Body Worn Cameras

October 1, 2021 – Sept. 30, 2022

Description	A description of all non-privileged and non-confidential information about use of the Surveillance Technology, including but not limited to the quantity of data gathered and sharing of data, if any, with outside entities. If sharing has occurred, the report shall include general, non-privileged and non-confidential information about recipient entities, including the names of the entities and purposes for such sharing. Body Worn Cameras are used to capture video recordings of contacts between department personnel and the public, to provide an objective record of these events. These recording are used in support of criminal prosecutions, to limit civil liability, increase transparency and enhance professionalism and accountability in the delivery of police services to the community. Body Worn Camera (BWC) files are shared with the Alameda County District Attorney's office in support of prosecution for crime, and may be shared with other law enforcement agencies to support criminal investigations. **Policy regarding activation of the Body Worn Camera BPD Policy 425.7** Members shall activate the BWC as required by this policy in (a)-(f) below, and may activate the BWC at any time the member believes it would be appropriate or valuable to record an incident within the limits of privacy described herein. The BWC shall be activated in any of the following situations: (a) All in-person enforcement and investigative contacts including pedestrian stops and field interview (FI) situations. (b) Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops. (c) Self-initiated field contacts in which a member would normally notify the Communications Center. (d) Any search activity, including the service of search or arrest warrants; probation, parole, or consent searches where the member is seeking evidence of an offense, or conducting a safety sweep or community caretaking sweep of the premises. Once a location has been secured and the member is not interacting with detainees or arrestees, the member may mute their BWC when conducting a search for evidence. (e) Any other contact that the member determines has become adversarial after the initial contact in a situation where the member would not otherwise activate BWC recording. (f) Transporting any detained or arrested person and where a member facilitates entry into or out of a vehicle, or any time the member expects to have physical contact with that person. **What data is captured by this technology:** BWC use is limited to enforcement and investigative activities involving members of the public. The BWC recordings will capture video and audio evidence for use in criminal investigations, administrative reviews, training, civil litigation, and other proceedings

<table>
<tr><td></td><td>protected by confidentiality laws and department policy. Improper use or release of BWC recordings may compromise ongoing criminal and administrative investigations or violate the privacy rights of those recorded and is prohibited.

How the data is stored:

BWC videos are stored on a secure server. All BWC data will be uploaded and stored on Axon Cloud Services, Evidence.com. Axon complies with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States (collectively, “Privacy Shield”). Axon has certified to the U.S. Department of Commerce that it adheres to the Privacy Shield Principles.

Retention period of data:

See attached retention schedule.

Summary of Body Worn Camera Videos Uploaded Oct. 1, 2021 to Sept. 30, 2022:

Total Number of Videos 64,688
Total Hours of Videos 17,520
Total GB of BWC Videos 30,420

Summary of Digital Evidence Uploaded, Oct. 1, 2021 to Sept. 30, 2022:

Type File Count
Audio 8,425
Document 1,804
Image 496,694
Other 2,807
Video* 79,303
Total 138,716

* Includes all uploaded BWC videos and all other videos booked into the evidence management system. Other videos include iPhone videos uploaded, security camera video, copies of BWC videos (for redaction, etc.), and any other videos.</td></tr>
<tr><td>Geographic Deployment</td><td>Where applicable, non-privileged and non-confidential information about where the surveillance technology was deployed geographically.

Body Worn Cameras are worn by all BPD uniformed officers city-wide at all times; BWC’s are not deployed based on geographic considerations.</td></tr>
<tr><td>Complaints</td><td>A summary of each complaint, if any, received by the City about the Surveillance Technology.

There have been no complaints about the deployment and use of Body Worn Cameras.</td></tr>
</table>

Audits and Violations	The results of any non-privileged internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response. File meta-data are routinely reviewed by our BWC manager, to ensure required metadata fields are completed. There have been no complaints with regards to violations of the Surveillance Use Policy.
Data Breaches	Non-privileged and non-confidential 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. There have been no known data breaches or other unauthorized access to BWC data.
Effectiveness	Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes. Body Worn Cameras have proven effective in supporting criminal prosecutions, as video footage is available for all criminal prosecutions. Body Worn Cameras have been effective for training purposes, as footage can be reviewed in incident de-briefs. Body Worn Cameras have been extremely effective in support of Internal Affairs investigations and Use of Force Review.
Costs	Total annual costs for the Surveillance Technology, including personnel and other ongoing costs. The annual cost for the Body Worn Cameras, including cameras, replacement cameras, software, and Axon's secure digital evidence management system is $222,442 per year over a five-year, $1,112,213 contract. There is one full-time employee assigned to the BWC program, an Applications Programmer Analyst II, at a cost of $168,940 per year, including benefits.

Surveillance Technology Report: Global Positioning System Tracking Devices

October 1, 2021 – Sept. 30, 2022

Description	A description of all non-privileged and non-confidential information about use of the Surveillance Technology, including but not limited to the quantity of data gathered and sharing of data, if any, with outside entities. If sharing has occurred, the report shall include general, non-privileged and non-confidential information about recipient entities, including the names of the entities and purposes for such sharing. Global Positioning System Trackers are used to track the movements of vehicles, bicycles, other items, and/or individuals. **What data is captured by this technology:** A GPS Tracker data record consists of date, time, latitude, longitude, map address, and tracker identification label. The data does not contain any images, names of subjects, vehicle information or other identifying information on individuals. **How the data is stored:** The data from the GPS tracker is encrypted by the vendor. The data is only accessible through a secure website to BPD personnel who have been granted security access. **Retention period of data:** Tracker data received from the vendor shall be kept in accordance with applicable laws, BPD policies that do not conflict with applicable law or court order, and/or as specified in a search warrant. The Global Positioning System "Electronic Stake Out" (ESO) devices were not deployed during this reporting period. This program was suspended in mid-March 2020 due to the COVID-19 pandemic. In June of 2022, we renewed our service with the company and paid for new updated equipment with the intent of restarting the program. The program was not reimplemented during the dates specific to this report. GPS "Slap-N-Track" (SNT) devices were used in three separate investigations during this reporting period: (1) An investigation into individuals for their involvement in shootings that occurred in Berkeley. The case resulted in the arrest of two individuals involved in the shootings and the recovery of 2 rifles and 4 handguns. (2) An investigation into individuals involved in a shooting that occurred in Berkeley. The case resulted in 2 individuals being arrested for their involvement in the shooting and the recovery of gun parts, ammunition and various drugs. (3) An investigation into an armed robbery and shooting that occurred in Berkeley. The case resulted in the recovery of 1 shotgun, 2 handguns and drugs. The suspect currently has an outstanding warrant for his arrest. Data may be shared with the District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence; other law enforcement

	personnel as a part of an active criminal investigation; and other third parties, pursuant to a court order.
Geographic Deployment	Where applicable, non-privileged and non-confidential information about where the surveillance technology was deployed geographically. GPS SNT devices are deployed with judicial pre-approval, based on suspect location, rather than geographical consideration.
Complaints	A summary of each complaint, if any, received by the City about the Surveillance Technology. There were no complaints made regarding GPS Trackers.
Audits and Violations	The results of any non-privileged internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response. There were no audits and no known violations relating to GPS Trackers.
Data Breaches	Non-privileged and non-confidential 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. There were no known data breaches relating to GPS Trackers.
Effectiveness	Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes. The GPS ESO trackers were not used during this time period. The program was suspended in mid-March 2020 due to the COVID-19 pandemic. Our subscription was renewed and we upgraded our equipment. We have not used them during this reporting period. GPS SNT trackers are effective in that they provide invaluable information on suspect vehicle location during the investigation of complex cases where suspects may be moving around the Bay Area and beyond. GPS Trackers greatly reduce costs associated with surveillance operations. A bike may be left for days. Surveillance operations generally involve four or more officers for the entire duration of an operation. A moving surveillance is extremely resource-intensive, requiring multiple officers in multiple vehicles for extended periods of time. Using both types of GPS trackers eliminates the need for officers' immediate presence until officers are ready to apprehend the suspect(s).
Costs	Total annual costs for the Surveillance Technology, including personnel and other ongoing costs. The annual cost for the GPS "Slap-N-Track" (SNT) data service is $1,800. The annual cost for the GPS "Electronic Stake Out" (ESO) devices this year was $2,353.85. This was to upgrade our devices and for three years of tracking service for the devices. There are staff time costs associated with preparing and placing SNT trackers. The investigator must prepare a search warrant and obtain a judge's approval, and a small number of officers must place the tracker on the suspect's car. The total number of hours

	is a fraction of the time it would take to do a full surveillance operation involving numerous officers. There are staff time costs associated with preparing ESO trackers and placing ESO tracker-equipped bikes for bait bike operations. These are on the order of two-four hours per operation. The total number of hours is extremely small, given the large number of operations, and resulting arrests.

Surveillance Technology Report: Automated License Plate Readers

October 1, 2021 – Sept. 30, 2022

Description	A description of all non-privileged and non-confidential information about use of the Surveillance Technology, including but not limited to the quantity of data gathered and sharing of data, if any, with outside entities. If sharing has occurred, the report shall include general, non-privileged and non-confidential information about recipient entities, including the names of the entities and purposes for such sharing. Automated License Plate Readers (ALPRs) are used by Parking Enforcement Bureau vehicles for time zone parking and scofflaw enforcement. The City's Transportation Division uses anonymized information for purposes of supporting the City's Go Berkeley parking management program. ALPR use replaced the practice of physically "chalking" tires, which is no longer allowed by the courts. **What data is captured by this technology:** ALPR technology functions by automatically capturing an image of a vehicle's license plate, transforming that image into alphanumeric characters using optical character recognition software, and storing that information, along with relevant metadata (e.g. geo-location and temporal information, as well as data about the ALPR). **How the data is stored:** The data is stored on a secure server by the vendor. **Retention period of data:** During this reporting period collected images and metadata of hits were stored no more than 365 days. Metadata of reads were not stored more than 30 days. Current use policy adopted September 13, 2022 sets new retention periods that are now in effect. **Summary of ALPR Time Zone Enforcement Data** Read Data (only retained for 30 days per prior policy) There was a total of 3,117,058 reads From 10/1/2021 to 9/30/2022 Hit Data There were 76,650 "Hits" 34,976 "Enforced Hits" resulted in citation issuance. 1,134 "Not Enforced" valid, enforceable hits resulted in no citation issued, based on PEO discretion. 40,540 Hits were not acted upon for a variety to reasons including but not limited to: 1) Customer comes out to move a vehicle. PEO's are directed not to issue that citation. 2) Officer gets to the dashboard and sees a permit not visible from a previous location.

	3) Officer does a vehicle evaluation and confirms that the vehicle moved from the hit location (e.g. across the street within GPS range). 4) Stolen car. 5) Similar Plates. 6) 600-700 GIG cars- 100 revel scooters. 7) Officers mistakenly leave their LPR "on" collecting time zone enforcement data, but leave the area being enforced to drive to another location on another assignment, such as a traffic post at a collision scene. These hits are not enforced. Genetec is the vendor for the ALPR Time Zone enforcement system. A "read" indicates the ALPR system successfully read a license plate. The information that is generated when a plate is viewed by the ALPR camera is the license plate number, state and geographical (GPS) location it was viewed. A "hit" indicates the ALPR system detected a possible violation, which prompts the Parking Enforcement Officer to further assess the vehicle. At "hit" is when the "read" information is recognized as a license plate that matches, or does not match an entry in a list such as permit list or the stolen vehicle "hot list". In many cases, hits are "rejected" or "not enforced", meaning no enforcement action is taken, because the Parking Enforcement Officer determines the vehicle has an appropriate placard or permit, or there is other information or assignment which precludes citation. **Summary of ALPR Booting Scofflaw Enforcement Data** 0 vehicles booted from 10/1/21-9/30/22 The Berkeley Police Department no longer maintains the ALPR Booting Scofflaw Enforcement Program. The contract to provide this service became cost prohibitive and the city opted not to renew the contract with the vendor. The city returned to having each PEO working a beat again become responsible for recognizing when a license plate has accumulated five or more unpaid parking tickets. **Summary of ALPR Law Enforcement Investigative Inquiry Data** 0 vehicle inquiries from 10/1/21-9/30/22 All BPD ALPR data may only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes, or as otherwise permitted by department policy and law. All ALPR data is subject to the provisions of BPD Policy 415 - Immigration Law, and therefore may not be shared with federal immigration enforcement officials.
Geographic Deployment	Where applicable, non-privileged and non-confidential information about where the surveillance technology was deployed geographically. Only Parking Enforcement Vehicles are equipped with ALPRs. ALPRs are deployed based on areas where there are parking time restrictions. ALPRs are not deployed based on geographic considerations not related to parking and scofflaw enforcement.

Complaints	A summary of each complaint, if any, received by the City about the Surveillance Technology. There have been no complaints about the deployment and use of Automated License Plate Readers.
Audits and Violations	The results of any non-privileged internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response. There have been no complaints of violations of the ALPR Surveillance Use Policy.
Data Breaches	Non-privileged and non-confidential 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. There have been no known data breaches or other unauthorized access to Automated License Plate Reader data.
Effectiveness	Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes. ALPRs have proven effective in parking enforcement for time zone enforcement. ALPRs have proven effective in supporting enforcement upon vehicles which have five or more unpaid citations. The ALPR's ability to read and check license plates while being driven greatly increases efficiency, allowing an operator to cover larger areas more quickly without having to stop except to confirm a hit.
Costs	Total annual costs for the Surveillance Technology, including personnel and other ongoing costs. The annual system maintenance cost for Genetec is $51,720. This cost is borne by the Transportation Division, which covers warranties, support, and cellular connection costs. Genetec ALPR units are installed on 22 Parking Enforcement vehicles. Parking Enforcement personnel perform a variety of parking enforcement activities, and are not limited solely to time zone enforcement. Therefore, personnel costs specifically attributable to time zone enforcement are not tracked.

Surveillance Technology Report: Street Level Imagery Project

October 1, 2021 – Sept. 30, 2022

Description	**A description of all non-privileged and non-confidential information about the use of the Surveillance Technology, including but not limited to the quantity of data gathered and sharing of data, if any, with outside entities. If sharing has occurred, the report will include general, non-privileged and non-confidential information about recipient entities, including the names of the entities and purposes for such sharing.** Street level imagery is utilized exclusively by authorized City staff for infrastructure asset management and planning activities. The street level imagery of City infrastructure assets in the Public Right of Way that is provided to the City will not consist of information that is capable of being associated with any individual or group.
Geographic Deployment	**Where applicable, non-privileged and non-confidential information about where the surveillance technology was deployed geographically.** Street level imagery was collected by driving through the entire community over a three week period. It is accessible to the City through a proprietary third-party application, Street SmartTM.
Complaints	**A summary of each complaint, if any, received by the City about the Surveillance Technology.** There have been no complaints about the use of Street Smart TM.
Audits and Violations	**The results of any non-privileged internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response.** There have been no complaints with regards to violations of the Surveillance Use Policy.
Data Breaches	**Non-privileged and non-confidential 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.** There have been no known data breaches or other unauthorized access to Cyclomedia Street Level Imagery data.

Effectiveness	**Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes.** Staff considered hiring contractors to use GPS in the field to create and update the infrastructure asset GIS data. This method is costly and time consuming. Cyclomedia's unique and patented processing techniques allow positionally-accurate GIS data to be collected in a cost-effective way and over a shorter period of time than a "boots on the ground" GPS field survey. The Imagery extracted the following Citywide Infrastructure assets to create accurate and current Geographic Information Systems (GIS) data inventories: • Bus pads / stops • Maintenance Access Holes • Pavement Striping • Curb paint color • Parking meters • Pedestrian Signal • Pavement marking • Storm drains • Signs • Street trees • Traffic lights The street level imagery captured was also being used to: Created a street sign GIS layer with condition assessment to support compliance with the Manual on Uniform Traffic Control Devices Code and provide an accurate inventory of City signs. The existing sign inventory is contained in a spreadsheet that does not have accurate location data. Created a curb color layer with condition assessment to indicate where there are red, yellow, blue, white and green colors. This is critical to support Public Safety. Created pavement striping and paint symbol layers to support Transportation Planning and Vision Zero. ***Benefits Projected:*** The data from the street level imagery is being integrated into the City's work order and asset management system for planning activities and to document repair and maintenance. Planners can use the street level imagery provided to the City to take measurements remotely, such as sidewalk width and public right of way impacts at proposed development locations. City staff can use the street level imagery to plan the location of road markings for pedestrian crossings, bike lanes or other striping.

<table>
<tr><td></td><td>City staff can remotely take accurate measurements of infrastructure assets to adequately plan for repair and replacement.

City staff can use street level imagery to enhance community engagement. The street level imagery can be used to identify and depict the impact of development such as an intersection restriping plan in order to article before and after conditions.</td></tr>
<tr><td>Costs</td><td>Total annual costs for the Surveillance Technology, including personnel and other ongoing costs.

The total cost of the system is $232,611 and is itemized below.
<table>
<tr><th>Year No.</th><th>Description</th><th>Cost</th><th>Notes</th></tr>
<tr><td>1</td><td>Licenses</td><td>$48,000</td><td>Resolution No: 69,482-N.S. 30JUN20</td></tr>
<tr><td>1</td><td>Professional Services for asset extraction</td><td>$139,401</td><td>Resolution No: 69,482-N.S. 30JUN20</td></tr>
<tr><td>2</td><td>Licenses and Support – One-Time</td><td>$41,100</td><td>Resolution No: 70,487-N.S. 26JUL22</td></tr>
<tr><td>3</td><td>License and Support – Ongoing Annual Costs</td><td>$4,110</td><td>Resolution No: 70,487-N.S. 26JUL22</td></tr>
</table></td></tr>
</table>

Surveillance Technology Report: Unmanned Aerial Equipment, Drone

October 1, 2021 – Sept. 30, 2022

Description	A description of all non-privileged and non-confidential information about use of the Surveillance Technology, including but not limited to the quantity of data gathered and sharing of data, if any, with outside entities. If sharing has occurred, the report shall include general, non-privileged and non-confidential information about recipient entities, including the names of the entities and purposes for such sharing. Unmanned Aerial Vehicle (UAV) also commonly referred to as a drone are requested pursuant to our Mutual Assistance protocols. If a situation arises wherein the safety to the community, officers, or the offender can be increased through the means of de-escalation (adding time and distance to the situation) a supervisor can make the request. All requests go to the Chief of Police and then escalate to the City Manager for final approval. During this period, on three occasions the Police Department sought mutual assistance for drones. **What data is captured by this technology:** Unmanned Aerial Vehicles are owned and operated by the respective agency. While each piece of equipment is unique, generally UAV's can both record video and audio, while transmitting the data to the operator, thereby qualifying as a piece of Surveillance Technology pursuant to BMC 2.99.020. **How the data is stored:** During this reporting period Alameda County Sheriff's Office (ACSO) assisted the Berkeley Police Department by providing drones on three occasions. Per their policy, ACSO retains images captured during a UAV mission if there is reasonable suspicion of criminal activity. BPD personnel would request that evidence from ACSO if it was needed in support of criminal activity. During this rating period no data was stored by BPD. The Department will set storage and retention periods in a Drone Use Policy. **Retention period of data:** During this rating period no data was stored by BPD. At this time the Berkeley Police Department does not intend to acquire this technology but is actively consulting with the City Attorney's Office regarding developing a Drone Use Policy. That policy, when complete, will include data retention. **Summary of Uses of UAV's** BPD Case 22-31368 (**USE OF UAV**) On 07/09/22 BPD officers responded to a robbery with gunfire at 2625 San Pablo Ave. The offenders fled into 1100 block of Carleton Street. Officers secured the perimeter and requested mutual assistance from the ACSO drone team. Officers were able to safely detain and arrest four suspects, and recovered four guns (2 ghost guns including a short-barreled rifle, and 2 Glock semi-automatic firearms- all loaded). *Subsequently the City Council was notified of the temporary use of surveillance technology in exigent circumstances.*

	BPD Case 22-35231 (**USE OF UAV**) On 08/02/22 BPD attempted to detain a person who was wanted in connection with a murder in another jurisdiction. The offender fled on foot from BPD officers. Officers secured a perimeter and requested mutual assistance including the request for a drone. ACSO responded and assisted BPD. With the assistance of the drone officers were able to locate the suspect in the 1100 block of Chaucer Street. No injuries were sustained by the officers. The offender had minor injuries as a result of jumping over fences while fleeing from BPD officers, however no injuries were sustained from the detention and arrest. *Subsequently the City Council was notified of the temporary use of surveillance technology in exigent circumstances.* Solano Stroll Event **(USE OF UAV)** On September 10, 2022, Berkeley and Albany hosted the Solano Stroll street event. Solano Stoll is a long-standing family event that draws tens of thousands to the Solano Avenue Street fair. At the request of Albany PD, the Alameda County Sheriff's Office Drone Team responded to conduct routine checks of the rooftops for potential shooting threats during the event. This was conducted to ensure the event was not targeted by an active shooter in public space, as was the case in Highland Park earlier in the year and a number of other locations in recent years. *Subsequently the City Council was notified of the temporary use of surveillance technology in exigent circumstances.*
Geographic Deployment	Where applicable, non-privileged and non-confidential information about where the surveillance technology was deployed geographically. One instance it was deployed in the area of 1100 block of Carleton Street. Another instance it was deployed in the 1100 block of Chaucer Street. The final deployment was along Solano Avenue from the Berkeley/Albany border on the west to The Alameda on the east.
Complaints	A summary of each complaint, if any, received by the City about the Surveillance Technology. The City received one complaint about the deployment and the use of Unmanned Aerial Vehicles (UAV), AKA Drones, specifically related to the Solano Stroll.
Audits and Violations	The results of any non-privileged internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response. The City received one complaint about the deployment of a drone at Solano Stroll not meeting the exigent circumstances threshold of the Surveillance Use Policy. At this time the Berkeley Police Department does not intend to acquire this technology but is actively consulting with the City Attorney's Office regarding developing a Use Policy. It is unclear from the ordinance whether an Acquisition Report is also appropriate so we began consulting with the City Attorney's Office on this matter last month.

Data Breaches	Non-privileged and non-confidential 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. There have been no known data breaches or other unauthorized access to any of the data from the Unmanned Aerial Vehicles (UAV), AKA Drones.
Effectiveness	Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes. In two instances the use of the Unmanned Aerial Vehicles (UAV), AKA Drones led to the safe apprehension of violent offender(s), and in one instance aided in the safe recovery of four firearms, including a short-barreled assault rifle. The final instance augmented the police in providing a safe environment for a large-scale public gathering and ensured a rapidly evolving situation could be addressed with speed and precision.
Costs	Total annual costs for the Surveillance Technology, including personnel and other ongoing costs. The annual cost for the Unmanned Aerial Vehicles (UAV), AKA Drones is zero as the uses were covered by the responding agencies under the Mutual Assistance agreement. The only costs associated is staff time at each respective incident, however no costs for the use of the technology was incurred.