CITY OF OAKLAND

Privacy Advisory Commission

December 1, 2022
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, Vice Chair **District 5 Representative**: Omar De La Cruz, **District 6 Representative**: Gina Tomlinson, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Henry Gage III **Mayoral Representative**: Jessica Leavitt*

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

Privacy Advisory Commission

December 1, 2022
5:00 PM
Teleconference
Meeting Agenda

---

1. Call to Order, determination of quorum

2. Review and approval of the draft October 6 meeting minutes

3. Open Forum/Public Comment

4. Federal Task Force Transparency Ordinance – OPD – US Marshals Services (USMS), Alcohol Tobacco Firearms (ATF)
    a. Review and take possible action on the draft memoranda of understanding with federal partners (MOU)

5. Surveillance Technology Ordinance – DOT – Mobile Parking Payment Proposal
    a. Informational Report by CSU Law Clinic – no action will be taken at this meeting

CITY OF OAKLAND

Privacy Advisory Commission

October 6, 2022
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, Vice Chair **District 5 Representative**: Omar De La Cruz, **District 6 Representative**: Gina Tomlinson, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Henry Gage III **Mayoral Representative**: Jessica Leavitt*

---

1. **Call to Order, determination of quorum**

Members Present: Suleiman, Brown, Hofer, Katz, Brown, De La Cruz, Leavitt, Oliver

Tomlinson joined after Call to Order.

Absent: Gage

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

This item was moved by Chair Hofer, second by Lou Katz and passed unanimously.

3. **Review and approval of the draft July 7 meeting and July 12 special meeting minutes**

A motion was made by Chair Hofer to adopt the minutes, second by Member Leavitt,
member Suleiman abstained.

The minutes were adopted.

4. **Open Forum/Public Comment**

There were no speakers during open forum/public comment.

5. **Bylaw Change regarding agendas and notice**
    a. Review and take possible action

This item is formalizing a policy that Mr. DeVries initiated, and Vice Chair Katz added a bit more substance to Mr. DeVries' recommendation and the decision was made to incorporate into the PACs bylaws. The revised bylaws were in the agenda packet with the highlighted changes in yellow.

Chair Hofer asked for comments or suggestions from the PAC members and requested comments from the public, there were none.

Chair Hofer made a motion to approve the bylaws change and a second was made by Vice Chair Katz.

Roll call of the vote:
D1 – Yes
D2 - absent
D3 – Yes
D4 -Yes
D5 yes
D6 - Yes
D7 – Yes
At-large - absent
Mayoral appointee – yes

Item was adopted

6. **Surveillance Equipment Ordinance – OPD – Automated License Plate Reader**
    a. Review and take possible action on the impact statement and proposed use policy

Automated License Plate Reader discussion went to Public Safety Committee, and they kicked it back to the Privacy Advisory Commissions (PAC) to work on the policy. The PAC has not discussed the merits of the policy because when the items was first introduced is when the PAC started reviewing annual reports, audits and other things that need to be done. After reviewing these items and with direction from the PSC, the PAC will begin working on the policy. The PAC has the authority to meet and make recommendations and that was the direction of the PSC. ALPR was added to the council agenda, and it was unclear on how the process will move forward.

OPD's general order which was submitted to the PAC and Vice Chair Katz also worked on a version which was included in the agenda packet. Chair Hofer emailed a version of what Vice Chair Katz completed to refine the general order in certain areas and that's an item that Chair Hofer proposed. The Chair

indicated that the version he proposed, and Vice Chair Katz's were in close agreement there may be a few differences and that's what needed to be discussed.

Chair Hofer indicated that we have technology that can't be audited, we have not been tracking third party access adequately or in compliance with state law, we have not been getting efficacy data because they don't track it, specific uses are always an item we look at, retention might be an item we focus on the most. These are the provisions the Chair and Vice Chair both looked at and tried to make more privacy and civil liberties friendly and perhaps more accountability friendly.

DC Lindsay indicated that she appreciates the template of the policy, however, she thought OPD should have an opportunity to allow her subject matter experts to comment on the document. She also advised that the software was not updated to track the data.

The PAC engaged in a discussion of the policy with members of OPD.

As written with a few changes as discussed, including the 30 day data retention Chair Hofer moved that the policy is forward to the City Council with a recommendation that they adopt the PAC version. A second was made by Member Tomlinson.

Role call vote:

D1 – yes

D3 yes

D4 yes

D5 yes

D6 yes

D7 – yes

Mayor - yes

Item carried unanimously.

Mr. DeVries suggested that the PAC consider the technology upgrades that OPD requested. It's short paragraph in the impact statement that covers maintenance, security patches and auditing functions. Member Brown stated that if we were to fund this, is there a possibility that we would receive a report in a certain timeframe. Chair Hofer stated that the ordinance requires audits and broader language under state law that requires OPD to maintain the records of access. The upgrade will require them to comply with their obligation to produce the information in the annual report.

The chair made a motion to the Council that they approve the $16k funding to allow auditing, maintenance upgrades and ensure that a vendor is selected that will comply with the city's ordinance requirements. Second by Member Oliver.

D1 – Yes

D2 – absent

D3 – yes

D4 – yes

D5 – yes

D6 – absent

D7 – yes

Mayor – yes

Motion passed.

Public Comment:

One person provided public comment.

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES (ATF),

AND

THE OAKLAND POLICE DEPARTMENT (OPD)

This Memorandum of Understanding ("MOU") is entered into by and between the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF") and Oakland Police Department ("participating agency") as it relates to the Oakland Crime Gun Enforcement Team (herein referred to as the "Task Force").

BACKGROUND

The Oakland Crime Gun Enforcement Team ("CGET") is primarily tasked with combatting violent crime in the counties of Alameda and Contra Costa by conducting both state and federal investigations with partner agencies targeting those involved in shootings, armed robberies, homicides, and armed narcotics trafficking.

AUTHORITIES

The authority to investigate and enforce offenses under provisions of this MOU are found at 28 U.S.C. § 599A , 28 C.F.R. §§ 0.130, 0.131, and 18 U.S.C. § 3051.

PURPOSE

The Task Force will perform the activities and duties described below:

a. Investigate violent offenders using crime gun intelligence
b. Investigate firearms related violent crime
c. Investigate firearms trafficking
d. Gather and report intelligence data gathered through the National Integrated Ballistic Information Network ("NIBIN")
e. Conduct undercover operations where appropriate and engage in other traditional methods of investigation in order that the Task Force's activities will result in effective prosecution before the courts of the United States and the State of California.

MEASUREMENT OF SUCCESS

The success of Task Force's investigative initiatives will be measured by the reduction of violent crime within the Area of Responsibility (AOR). These measurements would include, but is not

limited to, tracking the successful criminal prosecutions of shooters and their sources of crime guns (federal and state), NIBIN leads, firearm recoveries, firearm traces, and sharing crime gun intelligence (CGI).

PHYSICAL LOCATION

Officers/agents assigned to this Task Force by their employer shall be referred to as task force officers (TFOs). TFOs will be assigned to the ATF Oakland Field Office and will be located at 1301 Clay Street #670S, Oakland, CA 94612.

SUPERVISION AND CONTROL

The day-to-day supervision and administrative control of TFOs will be the mutual responsibility of the participants, with the ATF Special Agent in Charge or his/her designee having operational control over all operations related to this Task Force.

Each TFO shall remain subject to their respective agencies' policies, and shall report to their respective agencies regarding matters unrelated to this agreement/task force. With regard to matters related to the Task Force, TFOs will be subject to Federal law and Department of Justice (DOJ) and ATF orders, regulations and policy, including those related to standards of conduct, sexual harassment, equal opportunity issues and Federal disclosure laws.

Failure to comply with this paragraph could result in a TFO's dismissal from the Task Force.

PERSONNEL, RESOURCES AND SUPERVISION

To accomplish the objectives of the Task Force, ATF will assign 5 Special Agents to the Task Force. ATF will also, subject to the availability of funds, provide necessary funds and equipment to support the activities of the ATF Special Agents and officers assigned to the Task Force. This support may include: office space, office supplies, travel funds, funds for the purchase of evidence and information, investigative equipment, training, and other support items.

Each participating agency agrees to make available to their assigned task members any equipment ordinarily assigned for use by that agency. In the event ATF supplies equipment (which may include vehicles, weapons or radios), TFOs must abide by any applicable ATF property orders or policy, and may be required to enter into a separate agreement for their use.

To accomplish the objectives of the Task Force, the OPD agrees to detail up to 3 fulltime TFOs to the Task Force for a period of not less than two (2) years.

All TFOs shall qualify with their respective firearms by complying with ATF's Firearms and Weapons Policy.

SECURITY CLEARANCES

All TFOs will undergo a security clearance and background investigation, and ATF shall bear the costs associated with those investigations. TFOs must not be the subject of any ongoing investigation by their department or any other law enforcement agency, and past behavior or punishment, disciplinary, punitive or otherwise, may disqualify one from eligibility to join the Task Force. ATF has final authority as to the suitability of TFOs for inclusion on the Task Force.

DEPUTATIONS

ATF, as the sponsoring Federal law enforcement agency, may request at its sole discretion that the participating agency's TFOs be deputized by the U.S. Marshals Service to extend their jurisdiction, to include applying for and executing Federal search and arrest warrants, and requesting and executing Federal grand jury subpoenas for records and evidence involving violations of Federal laws. Such requests will be made on an individual basis as determined by ATF.

A TFO will not be granted Department of Justice legal representation if named as a defendant in a private-capacity lawsuit alleging constitutional violations unless all deputation paperwork has been completed prior to the event(s) at issue in the lawsuit.

The participating agencies agree that any Federal authority that may be conferred by a deputation is limited to activities supervised by ATF and will terminate when this MOU is terminated or when the deputized TFOs leave the Task Force, or at the discretion of ATF.

ASSIGNMENTS, REPORTS AND INFORMATION SHARING

An ATF supervisor or designee will be empowered with designated oversight for investigative and personnel matters related to the Task Force and will be responsible for opening, monitoring, directing and closing Task Force investigations in accordance with ATF policy and the applicable United States Attorney General's Guidelines.

Assignments will be based on, but not limited to, experience, training and performance, in addition to the discretion of the ATF supervisor.

All investigative reports will be prepared utilizing ATF's investigative case management system, (N-Force) utilizing ATF case report numbers. The participating agency will share investigative reports, findings, intelligence, etc., in furtherance of the mission of this agreement, to the fullest extent allowed by law. For the purposes of uniformity, there will be no duplication of reports, but rather a single report prepared by a designated individual which can be duplicated as necessary. Every effort should be made to document investigative activity on ATF Reports of Investigation (ROI), unless otherwise agreed to by ATF and the participating agency(ies). This section does not preclude the necessity of individual TFOs to complete forms required by their employing agency.

Information will be freely shared among the TFOs and ATF personnel with the understanding that all investigative information will be kept strictly confidential and will only be used in furtherance of criminal investigations. No information gathered during the course of the Task Force, to include informal communications between TFOs and ATF personnel, may be disseminated to any third party, non-task force member by any task force member without the express permission of the ATF Special Agent in Charge or his/her designee.

Any public requests for access to the records or any disclosures of information obtained by task force members during Task Force investigations will be handled in accordance with applicable statutes, regulations, and policies pursuant to the Freedom of Information Act and the Privacy Act and other applicable federal and/or state statutes and regulations.

INVESTIGATIVE METHODS

The parties agree to utilize Federal standards pertaining to evidence handling and electronic surveillance activities to the greatest extent possible. However, in situations where state or local laws are more restrictive than comparable Federal law, investigative methods employed by state and local law enforcement agencies shall conform to those requirements~~, pending a decision as to a venue for prosecution~~.

The use of other investigative methods (search warrants, interceptions of oral communications, etc.) and reporting procedures in connection therewith will be consistent with the policy and procedures of ATF. All Task Force operations will be conducted and reviewed in accordance with applicable ATF and Department of Justice policy and guidelines.

None of the parties to this MOU will knowingly seek investigations under this MOU that would cause a conflict with any ongoing investigation of an agency not party to this MOU. It is incumbent upon each participating agency to notify its personnel regarding the Task Force's areas of concern and jurisdiction. All law enforcement actions will be coordinated and cooperatively carried out by all parties to this MOU.

INFORMANTS

ATF guidelines and policy regarding the operation of informants and cooperating witnesses will apply to all informants and cooperating witnesses directed by TFOs.

Informants developed by TFOs may be registered as informants of their respective agencies for administrative purposes and handling. The policies and procedures of the participating agency with regard to handling informants will apply to all informants that the participating agency registers. In addition, it will be incumbent upon the registering participating agency to maintain a file with respect to the performance of all informants or witnesses it registers. All information obtained from an informant and relevant to matters within the jurisdiction of this MOU will be shared with all parties to this MOU. The registering agency will pay all reasonable and necessary informant expenses for each informant that a participating agency registers.

DECONFLICTION

Each participating agency agrees that the de-confliction process requires the sharing of certain operational information with the Task Force, which, if disclosed to unauthorized persons, could endanger law enforcement personnel and the public. As a result of this concern, each participating agency agrees to adopt security measures set forth herein:

a. Each participating agency will assign primary and secondary points of contact.
b. Each participating agency agrees to keep its points of contact list updated.

The points of contact for this Task Force are:

ATF: The assigned ATF Assistant Special Agent in Charge/ASAC (primary) and the assigned ATF Resident Agent in Charge/RAC of the Oakland/CGET FO (secondary)

Participating Agency: Oakland PD Sgt. Steve Valle (primary) and Oakland PD Sgt. Seth Neri (secondary)

EVIDENCE

Evidence will be maintained by the lead agency having jurisdiction in the court system intended for prosecution. Evidence generated from investigations initiated by a TFO or ATF special agent intended for Federal prosecution will be placed in the ATF designated vault, using the procedures found in ATF orders.

All firearms seized by a TFO will be submitted for fingerprint analysis, DNA and/or for National Integrated Ballistic Information Network (NIBIN) examination as appropriate. Once all analyses are completed, all firearms seized under Federal law shall be placed into the ATF designated vault for proper storage. All firearms information/descriptions taken into ATF custody must be submitted to ATF's National Tracing Center.

JURISDICTION/PROSECUTIONS

Cases will be reviewed by the ATF Special Agent in Charge or his/her designee in consultation with the participating agency and the United States Attorney's Office and appropriate State's attorney offices, to determine whether cases will be referred for prosecution to the U.S. Attorney's Office or to the relevant State's attorney's office. This determination will be based upon which level of prosecution will best serve the interests of justice and the greatest overall benefit to the public. Any question that arises pertaining to prosecution will be resolved through discussion among the investigative agencies and prosecuting entities having an interest in the matter.

In the event that a state or local matter is developed that is outside the jurisdiction of ATF or it is decided that a case will be prosecuted on the state or local level, ATF will provide all relevant

information to state and local authorities, subject to Federal law. Whether to continue investigation of state and local crimes is at the sole discretion of the state or local participating agency.

USE OF FORCE

All fulltime TFOs will comply with ATF and the Department of Justice's (DOJ's) Use of Force orders and policies. TFOs must be briefed on ATF's and DOJ's Use of Force policy by an ATF official, and will be provided with a copy of such policy.

BODY WORN CAMERAS AND TASK FORCE OFFICERS

In accordance with DOJ policy, dated October 29, 2020, Body Worn Cameras (BWCs) may be worn by TFOs operating on a Federal Task Force when their parent agency mandates their use by personnel assigned to the task force. In such cases, the parent agency must formally request to participate in the TFO BWC program and, upon approval, shall comply with all DOJ and ATF policies, and the required procedures, documentation, and reporting while participating on the task force. This provision is only in effect when an Addendum to Task Force Agreements Pertaining to Body Worn Cameras is signed by the participating agency.

MEDIA

Media relations will be handled by ATF and the U.S. Attorney's Office's public information officers in coordination with each participating agency. Information for press releases will be reviewed and mutually agreed upon by all participating agencies, who will take part in press conferences. Assigned personnel will be informed not to give statements to the media concerning any ongoing investigation or prosecution under this MOU without the concurrence of the other participants and, when appropriate, the relevant prosecutor's office.

All personnel from the participating agencies shall strictly adhere to the requirements of Title 26, United States Code, § 6103. Disclosure of tax return information and tax information acquired during the course of investigations involving National Firearms Act (NFA) firearms as defined in 26 U.S.C., Chapter 53 shall not be made except as provided by law.

SALARY/OVERTIME COMPENSATION

During the period of the MOU, participating agencies will provide for the salary and employment benefits of their respective employees. All participating agencies will retain control over their employees' work hours, including the approval of overtime.

ATF may have funds available to reimburse overtime to the State and Local TFO's agency, subject to the guidelines of the Department of Justice Asset Forfeiture Fund. This funding would be available under the terms of a memorandum of agreement (MOA) established pursuant to the provisions of 28 U.S.C. section 524. The participating agency agrees to abide by the applicable Federal law and policy with regard to the payment of overtime from the Department of Justice Asset Forfeiture Fund. The participating agency must be recognized under State law as a law

enforcement agency and their officers/ troopers/investigators as sworn law enforcement officers. If required or requested, the participating agency shall be responsible for demonstrating to the Department of Justice that its personnel are law enforcement officers for the purpose of overtime payment from the Department of Justice Asset Forfeiture Fund. **This MOU is not a funding document.**

In accordance with these provisions and any MOA on asset forfeiture, the ATF Special Agent in Charge or designee shall be responsible for certifying reimbursement requests for overtime expenses incurred as a result of this agreement.

AUDIT INFORMATION

Operations under this MOU are subject to audit by ATF, the Department of Justice's Office of the Inspector General, the Government Accountability Office, and other Government-designated auditors. Participating agencies agree to permit such audits and to maintain all records relating to Department of Justice Asset Forfeiture Fund payments for expenses either incurred during the course of this Task Force or for a period of not less than three (3) years and, if an audit is being conducted, until such time that the audit is officially completed, whichever is greater.

FORFEITURES/SEIZURES

All assets seized for administrative forfeiture will be seized and forfeited in compliance with the rules and regulations set forth by the U.S. Department of Justice Asset Forfeiture guidelines. When the size or composition of the item(s) seized make it impossible for ATF to store it, any of the participating agencies having the storage facilities to handle the seized property agree to store the property at no charge and to maintain the property in the same condition as when it was first taken into custody. The agency storing said seized property agrees not to dispose of the property until authorized to do so by ATF.

The MOU provides that proceeds from forfeitures will be shared, with sharing percentages based upon the U.S. Department of Justice Asset Forfeiture policies on equitable sharing of assets, such as determining the level of involvement by each participating agency. Task Force assets seized through administrative forfeiture will be distributed in equitable amounts based upon the number of full-time persons committed by each participating agency. Should it become impossible to separate the assets into equal shares, it will be the responsibility of all the participating agencies to come to an equitable decision. If this process fails and an impasse results, ATF will become the final arbitrator of the distributive shares for the participating agencies

DISPUTE RESOLUTION

In cases of overlapping jurisdiction, the participating agencies agree to work in concert to achieve the Task Force's goals and objectives. The parties to this MOU agree to attempt to resolve any disputes regarding jurisdiction, case assignments and workload at the lowest level possible.

LIABILITY

ATF acknowledges that the United States is liable for the wrongful or negligent acts or omissions of its officers and employees, including TFOs, while on duty and acting within the scope of their federal employment, to the extent permitted by the Federal Tort Claims Act.

Claims against the United States for injury or loss of property, personal injury, or death arising or resulting from the negligent or wrongful act or omission of any Federal employee while acting within the scope of his or her office or employment are governed by the Federal Tort Claims Act, 28 U.S.C. sections 1346(b), 2672-2680 (unless the claim arises from a violation of the Constitution of the United States, or a violation of a statute of the United States under which other recovery is authorized).

Except as otherwise provided, the parties agree to be solely responsible for the negligent or wrongful acts or omissions of their respective employees and will not seek financial contributions from the other for such acts or omissions. Legal representation by the United States is determined by the United States Department of Justice on a case-by-case basis. ATF cannot guarantee the United States will provide legal representation to any State or local law enforcement officer.

Liability for any negligent or willful acts of any agent or officer undertaken outside the terms of this MOU will be the sole responsibility of the respective agent or officer and agency involved.

DURATION

This MOU is effective with the signatures of all parties and terminates at the close of business on September 30, 2026.

This MOU supersedes previously signed MOUs and shall remain in effect until the aforementioned expiration date or until it is terminated in writing (to include electronic mail and facsimile), whichever comes first. All participating agencies agree that no agency shall withdraw from the Task Force without providing ninety (90) days written notice to other participating agencies. If any participating agency withdraws from the Task Force prior to its termination, the remaining participating agencies shall determine the distributive share of assets for the withdrawing agency, in accordance with Department of Justice guidelines and directives.

The MOU shall be deemed terminated at the time all participating agencies withdraw and ATF elects not to replace such members, or in the event ATF unilaterally terminates the MOU upon 90 days written notice to all the remaining participating agencies.

MODIFICATIONS

This agreement may be modified at any time by written consent of all participating agencies. Modifications shall have no force and effect unless such modifications are reduced to writing and signed by an authorized representative of each participating agency.

ADDITIONAL TERMS

No data shall be shared with other agencies for the purposes of pursuing criminal charges or civil enforcement against individuals for obtaining, providing, or supporting reproductive health care services, to ensure that the medical rights of residents of and visitors to Oakland, a sanctuary city, remain intact.

In accordance with California law, OPD shall not issue warrants for the arrest of, surrender a person in, California if the arrest/surrender is for an abortion-related crime, unless otherwise required by law

In accordance with California law, OPD shall refuse non-fugitive extradition of individuals for criminal prosecution for receiving, providing, or supporting reproductive health care services, to ensure that the medical rights of residents of and visitors to Oakland, a sanctuary city, remain intact.

SIGNATURES

_____/_____	_____/_____
LeRonne Armstrong Date	Patrick Gorman Date
Chief of Police	Special Agent in Charge, ATF
Oakland Police Department	San Francisco Field Division

ATTACHMENT 1

Standard Operating Procedures for Task Force Officer Body-Worn Camera Program

BODY-WORN CAMERA TASK FORCE OFFICER AGENCY CHECKLIST

Complete separate checklist for each agency employing task force officers that will use body-worn cameras (BWC). Attach additional sheets ifnecessary.

Date: _____

ATF Division	Task Force	State/Local Agency
Person Completing Checklist		
Name	**Phone Number**	**Email Address**

A. State & Local Legal Authority		
List and attach any state or local laws applicable to BWCs or impacting BWCs (e.g., open records laws, legal retention requirements, etc.); and other pertinent legal guidance (e.g., significant case law, State AG Opinions, etc.). If none, enter "N/A." Add additional rows as necessary.		
Title	**Cite**	**Comments**
B. TFO Parent Agency Policies		
List and attach any policy, procedure, or other written directive from the TFO's parent agency applicable to TFOs' use of BWCs. Include any union or other labor agreement requirements regarding BWCs applicable to TFOs. If none, enter "N/A." Add additional rows as necessary.		
Title	**Cite**	**Comments**

Answer the following questions, including any applicable citation (e.g., state or local law, agency policy, vendor contract, etc.).		
	C. BWC System	
1	Name/model of BWC used by agency? Attach technical specifications.	
2	Internal storage of recordings or external with a 3rd party vendor? If a 3rd party, identify the vendor, attach contract.	
3	Does the BWC system include a "buffer" or "pre-record" function, or a "post-record" function? If so, state the length of the buffer/pre-record and/or post-record, and whether it is audio only or both audio and video.	
4	Can the system be configured to give designated ATF personnel direct access to view and copy TFO recordings at the ATF office?	
5	Will ATF need specialized software or equipment to view recordings? If so, specify.	
6	Will ATF need specialized software or equipment to copy recordings? If so, specify.	
7	Does the system have an audit function that will identify persons who accessed, downloaded, or copied recordings?	
8	How will ATF cases be identified in the agency's system?	
9	What metadata can be obtained from BWC recordings?	
10	How long will recordings be preserved in the agency's system? Attach any agency retention schedule, and note whether it is mandated by state /local law or agency policy only.	
11	Does the BWC system allow restriction of BWC recording access to specific persons within the agency?	
12	How does agency handle inadvertent/accidental recordings?	
13	How does agency handle requests to delete BWC recordings?	
14	Will the TFO be able to charge the BWC and/or download/upload the recordings into the agency's BWC system at the ATF task force office?	
15	Does the BWC have a GPS function? If so, is the function available to the TFO, and what is the agency's policy regarding use of GPS? Can it deactivated on TFO BWCs?	

16	Does the BWC have a "live stream" capability? If so, is the function available to the TFO, and what is the agency's policy regarding use of "live streaming" with BWCs? Can it deactivated on TFO BWCs?	
17	Does the agency utilize facial recognition technology with BWC recordings?	
18	Provide an agency point-of-contact who can provide information regarding system security and protections, and location and security precautions of data storage facilities. ***Do not attach this information.***	

	D. BWC Use	
1	Are there any exceptions under agency policy to the requirement to record search warrant executions or arrests?	
2	What is the agency's policy regarding BWC recording of CSs?	
3	Does agency prohibit BWC recording in any specific situations? If so, list.	
4	Under agency policy, are there circumstances when a supervisor may direct the officer to record or not record?	
5	What is the agency's policy regarding citizen notification of BWC recording?	
6	If the TFO's BWC is inoperable does the agency's policy permit the TFO to participate in enforcement activities if a replacement is not readily available?	

E. Law Enforcement Access to BWC Recordings		
1	Are officers allowed to review BWC recordings before writing reports? Giving statements? • If so, are they allowed to view only recordings from their own BWC, or are they allowed view BWC recordings from other officers?	
2	If officers are allowed to review recordings are there any exceptions? If so list the exceptions, e.g., internal investigations, critical incidents (e.g., officer-involved shooting (OIS), use of deadly force, etc.)?	
3	Who in the parent agency will have access to TFOs' BWC recordings involving ATF/federal cases?	
4	Does agency restrict access to BWC recordings involving a critical incident (e.g., OIS)? If so, who has access in those situations?	
5	Will members of the parent agency be able to identify ATF cases in the BWC system? How?	
6	Does the agency require random or directed supervisory review/audit of officer videos for policy compliance or other issues? If so, will this include TFO recordings of ATF cases?	
7	Will non-law enforcement employees of the parent agency or municipality have access to ATF BWC recordings, e.g., IT? If so, are they CJIS-compliant (e.g., CJIS background checks)?	
8	Are officers allowed to make copies of BWC recordings, or must they obtain recordings from someone else within the agency?	
9	Are officers allowed to possess copies of recordings outside the police facility, or retain possession of copies for personal use?	
10	Does the agency have a policy prohibiting sharing of recordings outside of law enforcement for non-official reasons?	
11	Does the agency have a policy prohibiting the posting of BWC recordings to the Internet, social media sites, or the media for non-official purposes?	
12	Does the agency have a policy prohibiting officers from wearing or using privately owned BWCs or any other non-issued BWC?	
13	Do any other law enforcement entities or personnel have direct access to recordings, e.g., prosecutor's office?	

14	Does the parent agency investigate TFO-involved shootings (or other TFO-involved events involving death or serious injury), or is this done by another agency? If another agency: • Identify the agency. • Is there an agreement, policy, or protocol in place with the agency for handling these situations? If so, attach.	

	F. External Access to BWC Recordings	
1	How does the agency handle external requests for BWC recordings? • Criminal discovery, subpoenas? • Civil/administrative discovery, subpoenas? • Open record/freedom of information requests? • Media requests? • Union requests? Is there an agreement with the union regarding union disclosure of BWC recordings? If so, attach copy.	
2	If the agency uses a 3rd party vendor to store recordings: • is security of or access to recordings addressed in the contract? • are background checks of vendor employees addressed in the contract? If so, attach copy.	
3	How does the agency handle redaction of BWC recordings prior to public release?	

Addendum to Task Force Agreements Pertaining to Body Worn Cameras

This addendum supplements the agreement between the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and the Oakland Police Department, dated [Insert date of current Task Force Agreement], establishing the [Insert name of Task Force, if applicable]. Pursuant to the "Department of Justice Policy – Use of Body-Worn Cameras (BWC) by Federally Deputized Task Force Officers," dated October 29, 2020, the Oakland Police Department has advised ATF that it will require its deputized officers participating in the Task Force to use Body Worn Cameras (BWCs). This addendum governs that use.

The parties hereby agree to the following:

I. TFOs will adhere to the DOJ Policy, ATF's Standard Operating Procedures for Task Force Officer Body Camera Program, and other applicable ATF policies and procedures.

II. The Oakland Police Department confirms that prior to executing this agreement it has provided to ATF details regarding the BWC system and cameras, including the details of any system protections, and any state or local policies or laws applicable to the TFO's use of BWCs, including any retention policies as detailed in Attachment 1 – Agency Checklist.

III. Use of BWCs During ATF Federal Task Force Operations:

A. Deputized Task Force Officers (TFO) through the Joint Law Enforcement Operations (JLEO) Program will be allowed to wear and activate their recording equipment with BWCs for the purposes of recording their actions only during:

1. A planned attempt to serve an arrest warrant or other planned arrest; or
2. The execution of a search warrant.

B. TFOs are authorized to activate their BWCs upon approaching a premises or a subject, and must deactivate their BWCs when the scene is secured as determined by the federal supervisor on the scene as designated by the ATF.

1. For purposes of this agreement, the term "secured" means that the scene is safe and under law enforcement control.
2. In the event circumstances arise requiring additional law enforcement assistance to secure the scene, the TFO will end BWC recording when relieved from the scene by another law enforcement agency.
3. If there are unanticipated interactions with the public or other exigent circumstances, such as contentious or violent interactions that could lead to the use of force, TFO's will, if and when it is safe to do so, reactivate their BWC either before, during, or after a planned arrest or execution of a search or seizure warrant or order.

4. For the execution of a search warrant, BWCs should not be used for searches of property lawfully in government custody or control, or a search to obtain digital or electronic records executed by a third party, such as an electronic service provider or custodian of electronic records.

C. TFOs will follow the provisions set forth in this agreement for use of BWCs, and if the provisions of this agreement conflict with provision in the agency's policy for TFOs while serving on the ATF Federal Task Force, personnel will be subject to the laws, regulations, polices, and personnel rules applicable to their respective agencies. TFOs duties and assignment can be modified as needed during an operation, investigation, or activities of the Task Force to ensure the TFO is in compliance with federal, state, and local requirements.

D. TFOs may use BWCs in accordance with this policy anywhere they are authorized to act as a police or peace officer under state, local, territorial or tribal law.

E. TFOs may use only agency-issued and agency-owned BWCs. TFOs will not be allowed to use any privately owned BWC or other recording device of any kind.

F. In the event a TFO's BWC is not working or inoperable due to a technical problem or cannot be used due to physical damage, and, in the judgement of the Task Force supervisor, delaying the operation to repair or obtain a replacement BWC is not practical or would impair the operation, the TFO may participate in the operation without using a BWC.

G. Even when BWC use would be permissible in the circumstances set forth in Section III A above, TFOs are prohibited from recording:

1. Undercover personnel;
2. Confidential informants or confidential sources;
3. On-scene witness interviews prior to or after the operation;
4. Personnel using specialized investigative techniques or equipment; or
5. Actions by any non-law enforcement persons at the scene who are assisting law enforcement personnel prior to or after the operation.

H. Even when BWC use would be permissible in the circumstances set forth in Section III A above, TFOs are prohibited from activating their BWC if in the judgment of the ATF the cases involve:

1. National security (including international and domestic terrorism investigations or cases involving classified information);
2. Public corruption;
3. Medical facilities; or
5. Other sensitive investigations as determined by ATF.

I. Even when BWC use would be permissible in the circumstances set forth in Section III A above, TFOs shall not use BWCs to record any activities related to:

1. Specialized or sensitive investigative techniques;
2. In a sensitive area; or
3. An undercover or covert status on behalf of the ATF Federal Task Force.

IV. The Oakland Police Department Internal Controls:

A. [Insert Name of a high-ranking agency command official] will serve as a point-of-contact (POC) for ATF on BWC matters.

B. The Oakland Police Department will notify ATF of any change in state or local law that will modify how ATF TFOs must use BWCs or will affect release or redaction of BWC recordings from TFO BWCs made while working under federal authority on behalf of ATF ("TFO BWC recordings").

C. The Oakland Police Department will notify ATF of any change in agency policy that will affect the storage, release, or redaction of TFO BWC recordings.

D. The Oakland Police Department will familiarize ATF Task Force personnel on the BWCs, specifically concerning their capabilities and operation during task force activities.

V. Handling of BWC Recordings Made During Task Force Operations:

A. For purposes of this agreement, the term "TFO BWC recordings" refers to audio and video recordings, and associated metadata, from TFO BWCs made while the TFO is working under federal authority.

B. In accordance with current agency policy and practice, the Oakland Police Department will provide full, un-redacted copies of TFO BWC recordings to ATF within 72 hours unless approved in writing by the ATF SAC.

C. TFOs will document BWC use and the existence of BWC recordings in the Report of Investigation (ROI). The TFO will include in the ATF ROI a statement attesting that the data provided is a fair and accurate copy of the data recorded by the BWC.

D. All TFO BWC recordings made during ATF Federal Task Force operations, including such recordings retained by the Oakland Police Department and/or in the possession of any third party engaged by the Oakland Police Department to store or process BWC recordings, shall be deemed federal records of the United States Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives (DOJ/ ATF) pursuant to the Federal Records Act.

E. Internal Dissemination:

The TFO's parent agency is authorized to use TFO BWC recordings for internal investigations of its personnel consistent with the parent agency's policies and procedures, not involving dissemination outside the parent agency or public release. The parent agency shall provide written notification to ATF prior to any internal review.

F. Expedited Public Release:

All TFO BWC recordings made during ATF Federal Task Force operations are federal records and shall be retained and disseminated in accordance with all applicable federal laws, policies and procedures including the Federal Records Act, Freedom of Information Act, and/or the Privacy Act. All TFO BWC recordings made during ATF Federal Task Force operations will be provided to ATF. The Department will work to expedite the public release of BWC recordings depicting conduct resulting in serious bodily injury or death of another consistent with DOJ policies and subject to any redactions as appropriate. If a TFO parent agency plans to release TFO BWC recording(s) from a BWC issued by the parent agency that depict conduct committed solely by a TFO resulting in serious bodily injury or death of another, the TFO's parent agency shall notify ATF, providing as much advance notice as possible as to the time and manner of its release. Following the notification, the TFO's parent agency may release such recording(s), subject to any redactions as appropriate.

If a TFO parent agency plans to release TFO BWC recording(s) from a BWC issued by the parent agency that depict conduct committed solely by an ATF agent resulting in serious bodily injury or death of another, the TFO's parent agency shall notify and coordinate the release with ATF, providing as much advance notice as possible as to the time and manner of its release. Following the notification, the TFO's parent agency may release such recording(s), subject to any redactions as appropriate.

G. In all circumstances, TFO BWC recordings shall be treated as law enforcement sensitive information, the premature disclosure of which could reasonably be expected to interfere with enforcement proceedings, and as potential evidence in a federal investigation, subject to applicable federal laws, rules, and policy concerning disclosure or dissemination (including but not limited to 28 C.F.R. Ch. 1, Pt. 16, Subpart B, "Touhy", absent appropriate redaction prior to disclosure or dissemination). Accordingly, these recordings are deemed privileged absent appropriate redaction prior to disclosure and may be entirely exempt from public release under federal laws, rules and policies.

H. If a TFO BWC recording involves a use of force incident to include: a shooting incident, any incident involving serious bodily injury or death, or where any enforcement action by ATF resulted in the use of force or deadly force; physical assault or attempted physical assault on a Law Enforcement Officer; intentional damage to any facility, conveyance or any property owned by ATF, or involves another time-sensitive or urgent situation, the Oakland Police Department will provide ATF copies on an expedited basis, including during non-business hours. For purposes of this provision, use of force incidents include, but are not limited to, incidents utilizing intermediate weapons, i.e., TASERs, expandable batons, kinetic energy projectiles, emergency/improvised intermediate impact weapons, such as, a flashlight or radio; any use of force resulting in serious injury or death; canine bites resulting in penetration of human skin; and all shooting incidents.

I. The Oakland Police Department will provide witnesses as needed to authenticate TFO recordings in ATF cases.

J. The Oakland Police Department will inform ATF of the length of time TFO BWC recordings will be retained by the agency before deletion. The Oakland Police Department will honor any request by ATF to retain the TFO BWC recordings for a longer period of time.

K. The Oakland Police Department will notify ATF immediately of any unauthorized access to TFO recordings discovered by the agency.

L. The Oakland Police Department will cooperate fully with ATF in the investigation of any unauthorized access to or disclosure of TFO recordings, including providing ATF the name(s) of any agency personnel determined by the agency to be involved in unauthorized access, copying, or disclosure.

M. The Oakland Police Department failure to comply with any part of this addendum may result in immediate termination of the Task Force Memorandum of Understanding.

N. The Oakland Police Department will notify ATF as soon as possible regarding any request or demand for release or disclosure of TFO recordings, including but not limited to subpoenas, discovery demands or motions, open record/freedom of information requests, media requests, or union or other professional association requests.

_____

Signature of Special Agent in Charge Date

_____

Signature of Department Official Date

Memo

To: Oakland City Department of Transportation Director Michael Ford
CC: Brian Hofer, Chair, Oakland Privacy Advisory Commission
Authors: Sarah Behlke, Sharilyn Clark, Jessica Cohen, Zachary Jacobson and Katrice Williams
Date: 11/28/2022

Subject: Cleveland State University Data Privacy and Equity Clinic Recommendations re: Implementation of New Multi-Provider Parking Payment System

I. Executive Summary

We are an interdisciplinary team of students at Cleveland State University participating in the Data Privacy & Equity Risk Assessment Clinic.[1] We were asked by the Oakland Department of Transportation (DOT) and the Oakland Privacy Advisory Commission (PAC) to review and analyze under the City of Oakland's (City) Surveillance and Community Safety Ordinance (Ordinance), the proposed implementation of a multi-provider parking payment system (System) described in the July 7, 2022 draft Surveillance Impact Report (SIR) and Surveillance Use Policy (Use Policy) included in the Appendix.

Over the course of almost four months, we worked with our faculty team to identify and assess privacy and enforcement concerns associated with surveillance technologies in general and, more specifically, those being used as part of the System. We reviewed numerous documents provided to us by the DOT and PAC. We also met a number of times with DOT and PAC leadership. Our student team developed an understanding of the System DOT seeks to put into place as well as the privacy framework the City has developed over the years through city council ordinances and the creation of the PAC.

As a result of the process outlined above, we provide in this memorandum our analysis and recommendations focused on two issues:

(1) privacy concerns from data sharing with the parking payment providers (Providers); and
(2) equity concerns in deployment and enforcement of the Mobile Parking Payment system through the use of handheld and vehicle-mounted automatic license plate reader (ALPR) devices.

For issue one, our overarching recommendation is that the City should incorporate aspects of the California Consumer Privacy Act (CCPA)[2] to protect consumer information as data protection addenda to the agreements with the parking payment providers. Specifically, we

[1] Please note that this is an interdisciplinary course intended to prepare students from different backgrounds to understand the privacy and equity risks raised by surveillance technologies and to work with communities to identify and mitigate those risks. Students in the course are not authorized to practice law, and the analysis and recommendations provided in this memorandum do not constitute, and are not intended to constitute, legal advice. The PAC and DOT should consult with experienced counsel as appropriate before deciding whether to act upon information or recommendations provided in this memorandum.

[2] "CCPA" in this document will refer to the CCPA as amended by the CPRA with the CPRA's main provisions going into effect on January 1, 2023.

recommend that the City include contractual requirements as addenda to its Performance Service Agreements (PSAs) with the Providers to classify them as Service Providers (SPs) under the CCPA and impose the CCPA's Service Provider obligations on them. Additional recommendations on this issue are also found below as they relate to the contractual relationship between the Providers and the City.

For issue two, our main recommendation is that the City take reasonable measures to ensure the accuracy of citation information and improve processes for motorists to correct citation errors and ALPR misidentifications, particularly where they may lead to fines, referrals to the Department of Justice or other actions of serious consequence to the individuals in question. There are a number of additional recommendations found below that focus on equitable enforcement measures.

We submit these recommendations and analysis for your review and consideration. We will also be presenting them to the PAC at its December 1, 2022 meeting.

II. Process

The Data Privacy & Equity Risk Assessment Clinic took place during Cleveland State University College of Law's Fall 2022 Semester. Students participating in the clinic include: Sarah Behlke, Sharilyn Clark, Jessica Cohen, Zachary Jacobson and Katrice Williams. The clinic is led by CSU faculty Professor Brian Ray (Law) and Dr. Patricia Stoddard-Dare (Social Work) with advisory support from Brian Hofer (PAC Chair) and Ann LaFrance (Outside Expert). Students and faculty met weekly for approximately two hours each week beginning in late August.

The project presented by Mr. Hofer was to work with DOT on the proposed implementation of a multi-provider parking payment system described in the July 7, 2022 draft SIR and Use Policy (included as Appendix A to this memo). Members of the team met three times with Michael Ford on the DOT staff to learn more about the proposed system. The team also reviewed the following documents over the course of the semester:

- Documents related to the System:
    - A Draft Package from July 2022 of documents re: Mobile Payment Parking Systems:
        - Draft Proposed use policy, dated 7/7/2022
        - Draft Anticipated Impact Report, dated 7/7/2022
        - Draft Proposed Use Policy, dated 5/6/2021
        - Appendix A for Mobile Parking Payment System, dated March 2022 (this looks like the RFP that went out)
        - Appendix B - Providers Privacy Policies (Passport, Pay by Phone, ParkMobile, IPS Group, Honk Mobile)
        - Appendix C - Providers' User Terms and Conditions (IPS Group, Honk Mobile, Pay by Phone, Passport, ParkMobile)
        - Appendix D - Existing Professional Services Agreement Language
    - Executed ParkMobile Professional Services Agreement
    - Draft Mobile Parking App Professional Services Agreement language

    - Oakland Professional Services Agreement Sample
    - 2019 Dockless Mobility Data Sharing Recommendation to Adopt a Resolution (draft and final)
    - 2019 Dockless Mobility Data Sharing Resolution (draft and final)
    - Dockless Mobility Data Sharing Impact Report
    - Dockless Mobility Data Sharing Use Policy
- Documents related to enforcement:
    - Oakland Parking Enforcement Equity Analysis
    - Automated License Plate Reader Final Use Policy
    - Automated License Plate Reader Final Anticipated Impact Report
    - Bio of Brandon Green
    - Progressive Parking Initiative information and white paper
- Oakland Laws:
    - Oakland City Council Surveillance Ordinance
    - Oakland Privacy Advisory Commission Bylaws
    - Oakland Privacy Advisory Commission Establishing Ordinance
    - Oakland Citywide Privacy Principles

These meetings and documents formed the basis for our understanding of the project as well as our analysis.

The student team developed a draft data map that attempted to visualize how the program would share information and how it would interact with the already existing parking enforcement efforts. This data map is provided as Appendix C. Ann LaFrance gave a detailed summary of relevant CCPA provisions to provide background information on data privacy requirements and best practices in California. Her slide deck is also included as Appendix B.

In conversations with Mr. Michael Ford, DOT's Parking and Mobility Division Manager, we learned that DOT began the procurement process for the System in order to receive payment and data from multiple Provider applications. DOT previously identified six Providers who meet the initial criteria for the project based on their responses to a Request For Proposals. DOT will enter into agreements with up to six of those Providers whose services will allow motorists to pay for parking sessions through a smartphone application, website, or text message. DOT would like to have multiple Providers to encourage competitive parking prices and give motorists some agency over their parking and privacy choices.

As a result of the process outlined here, and given timing and information constraints, we honed our analysis to focus on two areas of primary concern: (1) privacy concerns arising from data sharing with the Providers; and (2) equity concerns in the deployment and enforcement of the System through the use of handheld and vehicle-mounted ALPR devices.

III. Background

The City has in place an Ordinance that establishes a framework for reviewing the procurement and use of new surveillance technologies. The Ordinance amended the Oakland Municipal Code to require PAC review of new surveillance technologies (as defined in the

ordinance) before City Council approval. The PAC review requires a City agency requesting to implement a new surveillance technology or system to submit a SIR and a Use Policy. These documents must be reviewed and approved by the PAC before being submitted to the Oakland City Council for review. Only then can surveillance technology be adopted for use by the City.[3]

The Ordinance also requires the agency using the surveillance technology to prepare an Annual Surveillance Report and submit it to the PAC and City Council. A violation of the Ordinance or of a Use Policy constitutes an injury. Further, any person who has been subjected to a surveillance technology in violation of the Ordinance or whose information is used in violation of the Ordinance or of a Use Policy has a private right of action and is entitled to recover actual damages.[4]

In July 2022, DOT submitted to the PAC Chair, Brian Hofer, a draft SIR and Use Policy for a proposed Mobile Parking Payment System ("System") using up to six private payment providers ("Providers") whose services will permit individuals to pay for parking sessions through a mobile phone application ("app"), website, or text message in Oakland. These Providers are: ParkMobile, Oakland Parking Solutions, PayByPhone, Passport, Honk Mobile, and IPS Group. DOT plans to enter into agreements with the Providers that will permit individuals in Oakland to pay for their parking sessions through these Providers and for the Providers to collect and share data, including personal information, related to parking transactions with DOT through online portals for parking planning and enforcement. Specifically, DOT plans to use this parking data to analyze parking revenues and demand, to reconcile parking payments, to enforce parking restrictions, such as time limits and meter payments, to identify "scofflaws" who repeatedly fail to pay parking citations and to review citation disputes.

DOT had identified these six Providers from responses to an earlier request for proposals that meet the initial criteria. Once final PSAs are completed, those Providers who can meet the contractual requirements will be invited to contract with the City to provide services in connection with this System. We attempted to collect and review each of the six Providers' published privacy policies to analyze how each would use that information and comply with the CCPA). We were able to find the published privacy policies on the websites of all of the Providers with the exception of Oakland Privacy Solutions. In analyzing the Providers' publicly available privacy policies in light of CCPA, we could not easily identify how each Provider, based on their privacy policies alone, would treat either individual consumer information it collects in relation to the System or the other information DOT requires.

DOT plans to enter into agreements with each Provider that will require them to adhere to the final SIR and Use Policy. Our understanding from the draft agreement and discussions with DOT is that the City plans to restrict the ability of the Providers to use the information they

[3] It should be noted also that the City adopted Privacy Principles in 2020 as detailed in Oakland City Council Resolution 88071. Here, the City publicly declared its commitment to privacy as a "fundamental human right" and to "protect civil liberties." Additionally, the principles call for the City to "handle personal information in a manner that builds trust and preserves privacy and safety for residents, visitors, and members of the public."

[4] This description of enforcement is not intended to be a legal interpretation of the Ordinance, but rather a high-level summary of the Enforcement section of the Ordinance (9.64.050) so as to serve as a foundation for the analysis and recommendations that follow.

collect from motorists on behalf of the City. The draft Agreement states that ownership rights in any data collected by Service Providers shall vest in the City. This includes data from parking transactions created by the use of Service Providers' applications and stored by each Service Provider on its platform. The City's access to raw data should be restricted to limited City staff, as laid out in the City's Use Policy.

We were not able to definitively identify all of the information that the Providers will collect from motorists. In discussions with DOT, we learned that the description in the draft SIR and Use Policy of what data the Providers will collect and how that information will be shared with the City is still in development, although for our purposes we could assume the lists included in the SIR and Use Policy are final. In addition, the terms of the agreement that the City will enter into with each Provider and the restrictions it will include on data use and sharing are still under discussion. This memo draws on the existing draft documents we reviewed, supplemented by conversations with DOT. Many of our recommendations below focus on clarifying the personal information and other data that the Providers will collect and share, and limiting their use of that information.

As per the draft SIR and Use Policy, DOT will receive parking data from the Providers to analyze parking revenue and demand, reconcile payment disputes, and enforce parking restrictions.[5] According to the draft SIR, Providers will collect data including individual user account details, consumer license plate, transaction date, start and stop times, fees, and corresponding parking zones.[6] From our discussions with DOT, this information will be used for two general purposes: (1) parking enforcement (including citation appeals); and (2) long-term parking planning.

According to the draft language for inclusion in the PSAs, Providers will be prohibited from using the data they collect on behalf of the City for any purpose other than to "provide functionality of the Service Provider's platform" (an undefined concept), to share data as directed by the City, and to comply with the agreement.[7] Other language in the SIR and Use Policy states that the City's data (undefined in the draft) will be stored in Service Provider data centers offsite from the City, and the City will rely upon the security and expertise of the Service Providers to keep the data secure.[8] The City understands this to be an issue between the Service Providers and their chosen third parties, and wishes to absolve itself of liability.[9] Nowhere does language restrict the Providers from using other information collected from motorists who use the System in any way they choose. The primary concerns related to the City's proposed contracts with the Providers is that the data protection provisions are very broad and do not seem to place appropriate limitations on their ability to use personal information collected on behalf of the City for their own business purposes, or share the data with third parties that are subject to the same limitations.

[5] Draft Mobile Parking App Language for PSA_MFord
[6] *See* "Draft Mobile Parking Payment Systems Proposed Use Policy," p. 1
[7] *See* Appendix G
[8] *Id.*
[9] *Id.*

As a part of the parking system, the City of Oakland intends to implement "demand responsive" parking zones with varying parking fees.[10] Parking signs will include a public-right-of-way that will direct motorists to a webpage with all available Providers and give agency to motorists to choose a Provider.[11] Each block within parking zones will have a unique zone number that is universal across all service providers and is also posted on new parking signs.[12] Zone numbers will correspond with city provided Facility IDs.[13] DOT intends to implement this mobile parking payment system in the Montclair Business District with eventual expansions into Chinatown and downtown Oakland.[14] Verification of parking sessions will be confirmed by the City's automatic license plate readers (ALPRs).

The PAC previously approved a proposed Use Policy[15] and surveillance impact report (SIR) (called Anticipated Impact Report in the document)[16] for the vehicle-mounted ALPRs for parking management and enforcement. Both address the use and deployment of ALPR devices. Under that Use Policy, trained DOT parking control technicians (PCTs) are authorized to use handheld (Zebra TC75X) and vehicle-mounted ALPR (Genetech's AutoVu) devices to verify valid parking sessions for motorists parked in commercial districts, city-owned parking garages, and residential permit parking (RPPs) areas.[17] DOT confirmed in a November 17, 2022 meeting that the city has purchased two additional vehicle-mounted ALPR devices, bringing their total city-owned parking enforcement vehicles with the ALPR mobile scanning devices to seven.[18] The vehicle-mounted ALPRs use external cameras to capture still images of license plate numbers, which are converted into metadata.[19] DOT uses optical character recognition to transform the metadata into a collection of alphanumeric codes for use amongst the Department and with approved third-parties, like Conduent.[20]

Conduent, a third party vendor, stores, safeguards and deletes the metadata received by the ALPR system according to state-wide regulatory standards.[21] It is responsible for storing the pure metadata collected in still images in a restricted access database.[22] The license plate

---

[10] Supra note 7, p. 2
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] *See* Proposed Use Policy for Vehicle-Mounted Automated License Plate Recognition (ALPR) for Parking Management and Enforcement.
[16] *See* Final Anticipated Impact Report for Vehicle-Mounted Automated License Plate Recognition (ALPR) for Parking Management and Enforcement
[17] *See* "Appendix A" of "Draft Proposed Use Policy: Mobile Parking Payment Systems for Parking Management and Enforcement." Section 1.1 – Technical Requirements and System Integration describes the system requirements for the third-party mobile payment providers, and requires their systems to fully integrate with current parking enforcement handhelds (Zebra TC75X), which can scan license plates for an active parking session and issue a citation if there is a parking violation, and the vehicle-mounted ALPRs (Genetech's AutoVu), which scans license plates along the streets that the vehicle travels.
[18] Michael Ford, Parking and Mobility Division Manager for DOT, confirmed in a November 17, 2022 meeting that since the publication of the AIR for mounted ALPRs the city has seven, instead of five, City-Owned Parking Enforcement vehicles. See *Supra note* 17, p. 2.
[19] *Supra note* 17
[20] *Id.*
[21] *Id.*, p. 3
[22] *Id.*

numbers are run against an anonymized list to determine if there are active parking violations and "hits."[23] Those that are not "hits" are simply classified as "reads."

Per the existing ALPR use policy, a license plate will result in a "hit" if it is located in an unpermitted zone, is committing a parking violation, lacks a valid parking session or residential permit or is on the "hotlist." A vehicle will be considered to be in an unpermitted zone if it is found to have an expired parking permit or none at all. Vehicles will appear on the "hotlist" if they are registered as stolen or if they are designated "scofflaw," which occurs when a motorist has collected five or more parking citations. License plates that are "hits" are stored for at least 90 days, the minimum time required under California law, and a maximum of five years per the City's Records Management Policy. The images and all identifying information from reads are automatically deleted after 24 hours. DOT is considering whether to continue to use a third-party to aggregate non-enforcement information the Providers will collect or to develop an alternative mechanism.

The primary equity concerns for the ALPRs relate to misidentification of scofflaw vehicles; correction measures for erroneously issued citations; considerations for improving the City's current payment plans to resolve citations; limiting data sharing of ALPR information with law enforcement; transparency and notice to motorists as to how their personal information will be used; and decreasing the penalties for unpaid parking violations on motorists' other driving privileges.

IV. Analysis and Recommendations

Part A: Data Sharing and Privacy Concerns

Recommendation 1: The City should include in its PSAs with Providers more specific restrictions modeled on the CCPA regarding how the Providers may use the data they collect as part of this system.

Data Sharing between the City and Parking Payment Providers

According to the draft SIR and Use Policy, DOT has identified the data being collected by the Providers under the City's instructions and shared with the City in either aggregate or individual form as including:[24]

- Consumer license plate (note: this data is necessary for DOT staff in the Parking Citation Assistance Center to respond to citation disputes)
- Transaction date
- Start and stop times

[23] *Id.*, p. 3. "Hits" are vehicles violating parking requirements, or those that are otherwise stolen and "scofflaw," as well as vehicles identified for booting and towing.

[24] The data fields listed here are based on the information we have received as of the writing of this memo. Without the draft contracts between the City and the Providers and the Statements of Work for each of the providers, the data fields listed may not be complete.

- User fee charged
- Parking (meter) fee charged
- Numerical zone corresponding to parking block

This data is referred to herein as "City Personal Information" (CPI). We modeled the flow of the data in a data map that is included here in Appendix C. As DOT indicated to us, the individual data listed above is disaggregated and will later be shared with Conduent, a third-party provider that enables enforcement.

As discussed in more detail in Recommendation 3 below, the Providers' own privacy policies state that they collect a range of other sensitive data from motorists not included in these fields. This was factored into our analysis.

Under the City's Surveillance Ordinance, the City is required to submit a Surveillance Impact Report and Surveillance Use Policy to the Privacy Advisory Commission prior to submitting the proposed existing surveillance technology to City Council for approval. Here, the City proposes to enter PSAs with up to six parking payment vendors who will be receiving and processing user data that will later become CPI. Those PSAs will incorporate the requirements for protecting data privacy and civil liberties in the SIR and Use Policy. The following recommendations consider the most effective way to safeguard CPI in those three documents.

California's Data Privacy Law - CCPA[25]

While there is no overarching national law governing data privacy, California has led the way in legislating the data protection obligations of entities doing business in the state. Among other things, the CCPA sets out the mandatory contract provisions that California businesses must include when sharing data with Service Providers and Third Parties, with the objective of protecting the personal information of all California residents.

As a government entity, the City is not subject to CCPA. Given the City's commitment to protecting data privacy and the requirements of the Ordinance, however, the City has a responsibility to ensure that those providing their personal information to these companies at the request of, and for use by, the City ("City Personal Information" or "CPI") have their data protected in accordance with the Ordinance and the City's Privacy Principles. The most effective way to protect individuals' data is to ensure that data protection best practices, in line with the relevant provisions of the CCPA, are included as contractual requirements in the PSAs negotiated with Providers by the City, as recommended below. Doing so is also consistent with the requirements set out in the Ordinance.

To elaborate, Article 4 of the draft regulations that area currently being finalized to implement the CPRA amendments to the CCPA provides as follows:

[25] As noted in the beginning of this memorandum the discussion of CCPA/CPRA in this section is for general informational purposes. It does not constitute, and is not intended to constitute, legal advice. The PAC and DOT should consult with counsel as appropriate before deciding whether to act upon information or recommendations provided.

§ 7050. Service Providers and Contractors.

(a) A service provider or contractor shall not retain, use, or disclose personal information Collected pursuant to its written contract with the business except:.
(1) For the specific Business Purpose(s) set forth in the written contract between the business and the service provider or contractor that is required by the CCPA and these regulations.

The CCPA requires Service Providers to adhere to a "business purpose" designation for data retention, use, and disclosure as described in a contract between the Service Provider and the "business."

The Ordinance requires City Council approval to enter into a "written agreement with a non-City entity to acquire, share, or otherwise use surveillance technology…including data sharing agreements" (Sec. 9.64.030.1) and requires the Surveillance Use Policy to specify how third-party data sharing should occur. Specifically, the Ordinance requires the Use Policy, at a minimum, to specify "[i]f and how other City departments, bureaus, divisions, 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."

Although the City is not technically subject to the CCPA, it would be advisable for the City to adopt the same contractual measures to protect personal information collected by the Providers on its behalf, as a matter of best practice. By enshrining these consumer protections in a data protection addendum to the PSA, the City would create a clear legal standard that should be used by City Departments when contracting with Service Providers and Third Parties. To ensure that the same contracting practices are followed in all such situations, these same requirements should be set forth in the relevant Use Policy.

Benefits of Contractually Requiring CCPA Classification of Providers

Those who park their cars in the City of Oakland are a captive audience. Given the choice of paying with coins or cash or using a parking payment provider, those who chose the payment providers have no choice but to submit their data to the vendor and hope it is protected correctly. The City therefore would be proceeding in a manner consistent with its Ordinance and Privacy Principles by ensuring the data are responsibly protected by third parties with which it contracts. The Providers, as private businesses, are presumably bound by the CCPA (assuming they meet the CCPA thresholds), even though the City is not itself covered by the CCPA since the City is a government entity. Given this, the City and the Providers should explicitly define their relationship and how they will use and protect CPI in the agreements the City will enter into with each Provider.

It is also worth noting that the pending CCPA (Sec. 999.314) regulations state that despite nonprofits and government agencies being excluded from the statutory definition of "business", vendors that provide services to nonprofits or government agencies will be deemed service providers if the vendor would otherwise meet the requirements and obligations applicable to service providers (this particular designation will be described *infra*). The Service Provider classification is likely to be perceived as advantageous from the Providers' perspectives, since

the CCPA imposes fewer regulatory obligations beyond those set forth in the contractual obligations mandated by the statute.

The following analysis discusses using the CCPA as a model to incorporate specific restrictions on the use and sharing of data in the Provider PSAs, ideally as a data protection addendum.[26] The CCPA classifies entities based on how they collect, use, and process customer data and imposes different obligations based on each category. Implementing the CCPA's scheme through the City's PSAs with each Provider will ensure that individuals using the City's parking facilities are subject to best practice data protections in the State of California, which would:

- Provide benchmarks for protecting personal information that is outsourced for processing
- Set clear limits regarding the sale or sharing of personal information
- Limit the use of personal information to business purposes specified by the City in the contract
- Restrict and clearly delineate the retention, use, and disclosure of the personal information outside of the direct business relationship between the parties
- Regulate how vendors combine personal information either directly or through business partners
- Set forth the parties' legal obligations regarding data retention, use, and disclosure
- Set forth the parties' ability to respond to security incidents and protect itself against illegal activity
- Establish the vendors' liability as limited to those of service providers as defined under the CCPA/CPRA
- Provide a legal framework within which the City can ensure residents and parkers that their personal information is protected
- Reassure users that the City has a vested interest in protecting their data/personal information which could be especially important if a company that has experienced a past data breach (e.g. ParkMobile) is chosen as a vendor

We note that including the CCPA requirements relating to Service Provider contracts as part of the City's PSAs with the Providers is fully consistent with the City's Privacy Principles and the Ordinance.

CCPA Requirements

Different provisions of the CCPA could apply depending on whether the Providers are classified as a "service provider" (SP), or a "third party" (TP). We recommend that the City incorporate the requirements for **service providers** under the CCPA into the Provider contracts**.**

The SP provisions in the CCPA/CPRA define a SP as an entity that processes personal information on behalf of a business, which the SP receives from or on behalf of the business and processes for a business purpose pursuant to a written contract. The SP designation providers more robust regulations by which the shared data is protected but also specifically characterizes

[26] As noted above, we are not providing legal advice. The City should consult with experienced privacy counsel if it decides to implement this recommendation.

the vendor's liability by minimizing the provisions of the CCPA applicable to Providers and limiting them to only regulations relating to SPs

Under this designation, SPs are prohibited from:

- Retaining, using, or disclosing the PI for any purpose other than the business purposes specified in the contract, including retaining, using, or disclosing the PI for a commercial purpose other than the business purposes specified in the contract with the business;
- Retaining, using, or disclosing the PI outside of the direct business relationship between the SP and the business;
- Combining the PI that the SP receives from, or on behalf of, the business with PI that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer.

This designation also allows for exceptions but limits the ability of the SP to retain, use, or disclose PI to very specific circumstances:

- To build or improve the quality of its services, provided that the SP does not use the PI of one business to perform services on behalf of another business.
- To detect security incidents and protect against malicious, deceptive, fraudulent or illegal activity.
- To comply with legal obligations, civil or criminal investigation, law enforcement, exercise or defend legal claims, etc.

This designation should be included in the PSA between the City and each Provider to ensure that the Provider adheres to the law and the City has recourse in the case of a data breach or other data security incident.[27]

Recommendation 2: Clarify the relationship between the Surveillance Impact Report (SIR), Data Use Policy, and the Provider PSAs

DOT provided us with draft language (in Appendix G) to be added to the standard City PSA for each provider, with the exception of ParkMobile as the PSA with ParkMobile was extended.. The draft language as it pertains to data privacy, merely refers to the "privacy requirements as set forth specifically in the [Statement of Work] and the Surveillance Impact Analysis." However, Section 1 of the draft SIR[28] describes a different data sharing system than the one DOT has indicated.

[27] These recommendations are based on the information regarding data fields that was available at the time of this writing. The CCPA categorizes providers as either SPs or Third Parties. This is based on the type of data and how it is being shared with the "business." A provider could, under the CCPA, be classified as either or both. In this case, we recommend SPs and it is important to note that this recommendation is based on data being shared.

[28] It should be noted that the draft Anticipated Impact Report dated July 7, 2022 is the document referred to herein as the Surveillance Impact Report. Further, we presume that the document titled "Surveillance Impact Analysis" in the draft PSA language refers to the Impact Report dated July 7, 2022. When the language is finalized, this discrepancy should be rectified to use one consistent title for the Surveillance Impact Report.

As the PSA draft reads now, the SIR is the only document that expressly limits the Providers regarding data sharing. If that is the intent, then the SIR needs to be updated with accurate information. The Use Policy uses similar language to describe the flow of data, that, even if not controlling, should still be updated to reflect the accurate flow of the data to and from the DOT, Service Providers, intermediaries and any other City departments. DOT should also determine if it is sufficient for the PSA to simply cross-reference the SIR or the Use Policy. Overall, the City should consider including more specific restrictions regarding the ownership and use of data (as described in Recommendation 1) to ensure that the responsibilities and obligations of all parties are clear in this regard. The City also should ensure that the relevant information on data collection, data sharing and data flows (along with the contractual obligations discussed above) is consistently referenced (or cross-referenced) in the PSA, SIR, Use Policy, and Statement of Work for each Provider.

An additional concern is that the PSA draft language currently does not address how changes to the Use Policy or the SIR will be reflected in the contractual relationship between the Providers and the City. The PSA should include a requirement that Providers comply with any updates to the Use Policy and the SIR to ensure that ongoing data privacy requirements are met. Providers should be provided with a reasonable timeline within which to implement the changes.

Lastly, if the City includes the previously recommended contractual language to designate the Providers as SPs in its PSAs with the Providers, we also recommend highlighting this within the proposed Use Policy/SIR to be submitted to the Privacy Advisory Commission. A section could be added to the Proposed Use Policy entitled "Additional Data Protections". In this section, the City can explain how contractual addendums related to the CCPA enable the City to better protect personal information.

The City may also refer to the recommended CCPA terms in the PSA addendum to note that the SP designation will allow the City to monitor the SP's compliance with the PSA through measures, including, but not limited to, ongoing manual reviews, automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.[29] Also important to note is that, in line with CCPA best practices, if a SP subcontracts to other SPs to assist in processing of PI, it must do so pursuant to a written contract that binds the subcontractor to observe all of the above requirements. The City may be including an "Audit and Oversight" section of the Proposed Use Policy and, if preferred, the suggested language here can be included in that section instead of a new one.

Recommendation 3: The SIR should incorporate an analysis of the risks posed by the Providers' current privacy policies. In addition, the City should consider requiring each Provider to adopt privacy policies for this System that include the recommendations below.

Vendor Privacy Policies

[29] This language reflects the evaluation measures the CCPA details that may be included in agreements with SPs found in the definitions section of the law under the definition of "Service Provider."

After reviewing in depth all the privacy policies of each proposed Provider, our interdisciplinary team identified several general concerns regarding the integrity of data privacy, as well as some Provider specific concerns.

First, all of the Provider privacy policies use vague, nondescript language throughout the privacy documents. This language does provide the specific information required for motorists to make a fully-informed decision about how the Providers will share or protect their data.

Second, the privacy policies all fail to fully address third parties used by Providers. These policies do not describe what a third party is in layman's terms, nor do they go into depth about what third party services providers they are employing. An average citizen reading these privacy policies would not understand that Providers are sending their personal information to other companies to store data or to what companies the personal data is being sent.

The third area of concern regards the Providers' commitment to adhere to the relevant provisions of the CCPA. . The only Provider privacy policies to acknowledge the CCPA were Passport and Park Mobile. Our suggestion is to inform the other Providers of this act and the necessity of following these guidelines if they desire to work with the City. This should, at a minimum, be made clear in the Use Policy as well as the PSA data protection addendum.

A fourth area of concern is that the only Provider with a set data retention period is Honk Mobile. Every other Provider fails to provide an exact period for data retention, with most including a statement similar to the following from IPS, "We will retain your Personal Information for the period necessary to fulfill the purposes outlined in this Privacy Notice and according to our internal data retention policy, unless a longer retention period is required or permitted by law." This example exhibits more of the vague language within these policies and the danger of Providers keeping personally identifiable information for longer than necessary, infringing on the consumer's rights. This lack of stated retention period is also in conflict with desired retention period the DOT includes in the SIR and Use Policy. We strongly recommend discussing retention periods with each Provider and setting limitations on how long these vendors can retain consumer personal information collected on behalf of the DOT.

We note that there is no publicly available privacy policy for Oakland Parking Solutions. The websites for Mortimer Smythe, Marina Security and Oakland Parking Solutions all lacked visible data privacy policies. We encourage DOT to ensure there is an existing privacy policy for Oakland Parking Solutions before contracting with them. We also advise that there should be an existing privacy policy for Oakland Parking Solutions and that the company be required to publish their privacy policy for all potential motorists in Oakland to view.

After reviewing these privacy policies, we also noted that Honk Mobile, PaybyPhone and IPS include photos and videos in data collection. The Honk Mobile privacy policy mentions the company could possibly receive photos or videos of motorists with no context as to how and why these photos and videos are obtained. PaybyPhone reports in their privacy policy the possibility of obtaining photos of vehicles as they enter and exit parking facilities but does not provide information if drivers are captured in these photos. IPS also collects photos as part of conducting audits to test their equipment and reports that these photos could include license plate numbers

and people, depending on the time of the audit. Although IPS reports they do not note the license plate numbers, it is concerning that these photos with license plates and people are retained.

As noted above, these concerns reinforce the recommendation for DOT to address these shortcomings with the Providers and incorporate appropriate risk mitigation language in the PSAs with the Providers as appropriate. At a minimum, the SIR should incorporate an analysis of the risks posed by these policies. In addition, DOT should consider establishing minimum information to be contained in the privacy policies of all Providers setting out their role in collecting, using, sharing and otherwise processing personal information related to the System, in conformity with the PSAs, the final version of the SIR and theUse Policy.

Part B - Enforcement and Equity

Recommendation 4: Take reasonable measures to ensure the accuracy of citation information and improve processes for motorists to correct citation errors and ALPR misidentifications.

When the handheld (Zebra TC75X) and vehicle-mounted ALPR (Genetech's AutoVu) devices are used by parking control technicians (PCTs), they may not transmit accurate information and can lead to erroneous parking citations or misidentified scofflaw or stolen vehicles. The devices scan vehicles' license plates and verify an active parking session or a current residential parking permit with ParkMobile, after the data has been anonymized by another independent third-party vendor, Conduent, which manages the tracking and issuing of citations.[30] ParkMobile provides information that allows PCTs to enforce parking restrictions, including time limits and meter payments; identifying scofflaw vehicles; issue citations for parking violations; and submit information to the Parking Citation Assistance Center staff to review citation disputes.[31] If there is an active session, the technicians are prohibited from issuing a citation.[32] However, if there is a "hit" for a scofflaw, abandoned, or stolen vehicle, as identified by Conduent, the information will be reported as a stolen vehicle to the appropriate law enforcement agency. Scofflaw vehicles will be reported to Paylock, the city's third-party vendor for "booting" scofflaw vehicles.[33]

The vehicle-mounted ALPR technology automates the processing of vehicle license plate and compliance information by using specially designed cameras to capture digital images from surrounding vehicles as they drive through commercial districts, RPPs and city-owned parking facilities.[34] The images are transformed into alphanumeric characters with specialized software and the stored images, plate information and related metadata are put in a restricted-access database.[35] After the information is stored, the transformed license plate characters are compared to databases of license plates of interest to operators.[36] There may be other backend server processes, intersystem communications, and various user interfaces like public self-serve

[30] *See* "Draft Anticipated Impact Report: Mobile Parking Payment Systems for Parking Management and Enforcement." p. 1
[31] *See* "Proposed Use Policy: Mobile Parking Payment Systems for Parking Management and Enforcement."
[32] *Id.*
[33] *Supra note* 17, p. 3
[34] *Id.* p. 1
[35] *Id.*
[36] *Id.*

applications to pay and resolve citations, as well.[37] The still images and metadata may potentially be shared with other third parties, including Conduent (the third-party parking citation issuer), ParkMobile (a parking payment processor), IPS (a single-head and multi-space smart meter) and Scheidt & Bachmann (a vendor handling off-street parking and an access control system) for "hits."[38]

"Hits" are vehicles violating parking requirements, or those that are otherwise stolen and "scofflaw," as well as vehicles identified for booting and towing.[39] Scofflaw vehicles are cars that have accumulated five or more citations in the last 30 days.[40] "Hits" can be shared with the Oakland Police Department, California DMV, other law enforcement agencies, and other cities' jurisdictions to support evidence of parking violations.[41] This creates significant equity concerns for Oakland residents and visitors, and business employees for a variety of reasons, including the erroneous issuance of parking violations and misidentification of motorists as "scofflaw" because of malfunctioning vendor payment applications that make it difficult to pay for parking.

Individuals of low socioeconomic status and with multiple responsibilities may not have the financial and/or resources to resolve misidentified scofflaw, and citations that were erroneously issued. For example, following a recent update to a ParkNYC mobile app for street parking, when the app was offline, New York City parkers were unexpectedly required to pay meters, many of which were non-functioning and required coins. During the delay, one parker received a pair of tickets costing $65 each.[42] Other parkers needed to create new user accounts on the mobile app, suffered long delays in receiving verification codes, and became subject to a new 20-cent-per-transaction fee, all of which delayed payment for their parking sessions. This is exclusive of users having difficulty accessing money from a previous version of the app, adding money to their virtual wallets, and being locked out of their accounts.

With DOT potentially adding five new third-party payment providers, there is a possibility that users will erroneously experience expired parking sessions,[43] app

[37] *Id.*
[38] *Id.* p. 5
[39] *Id.* p. 2
[40] *Id.*
[41] *Id.* p. 3
[42] Jose Martinez, *Parking App Glitches and New 20-Cent Fee Miff Motorists*, The City NYC, (October 20, 2022, 9:45 A.M.)
[43] A Columbus man using ParkMobile for a parking session received a $81 parking citation while visiting Ohio State University's campus. He paid for a visitor's spot from 7:23 to 8:23 a.m. on the morning of May 27, but by 8:11 a.m. he received a parking violation from OSU's parking enforcement agency, CampusParc. On June 2, 2022, the same thing happened again when he received another parking citation after paying for an hour session. OSU's operations and enforcement teams reported there were no issues with data transfer from ParkMobile payments to CampusParc's system. Eventually, CampusParc said the citations were erroneously issued because of one error by the enforcement officer and, the second, by the motorist incorrectly entering his license plate number into ParkMobile. J. Bullock, *Problems with new Columbus parking apps?*, NBC4i.com, (June 21, 2022, 6:02 P.M.)

dysfunctionality,[44] overdrawn bank accounts,[45] and being locked out of their accounts. This, in turn, could cause vendors to erroneously cause PCTs to issue expensive citations, which some people may have difficulty paying in a compressed time frame. This is an equity issue since residents with lower economic resources could be disproportionately harmed by errors in citation issuance and misidentifications.

Misidentification occurs when the data provided to an ALPR is inaccurate, and causes an individual's vehicle to be improperly recognized as a scofflaw and/or stolen vehicle, leading to improper government action against the licensed vehicle driver.[46] In one instance, a San Francisco police pulled over, arrested, and searched Denise Green, an African American city worker, because her car was misidentified as stolen due to a license plate reader error.[47] A separate Brennan Center report referenced the high error rates on ALPRs due to inaccurate hot lists and reads.[48] If hot lists are not updated, individuals can be mistakenly pulled over. A randomized control trial in Vallejo, California, found that 37 percent of all ALPR "hits" from fixed readers and 35 percent of hits from mobile ALPRs were misreads. And, in a parking enforcement white paper[49] provided by Mr. Ford, 13% of survey respondents noted that parking app malfunction was a pain point for their parking experience. DOT has not specified the processes that it has (or will) put in place to confirm the accuracy of the match, or the mechanisms for individuals to correct misidentifying information before any action is taken, other than to dispute citations with the assistance center staff.[50] This resolution is insufficient if the error lies with the vendor. Moreover, DOT has mentioned in the anticipated impact report for

[44] The municipality of Royal Oak recently switched its downtown parking meter system, with the Metro Parking Services Inc. vendor, which owns and operates the 800 metered spots in Royal Oak and mails parking violations to motorists. The large kiosk meters have cameras that photograph the license plates of parked vehicles. However, the new system immediately had issues with its meters, inaccurate fine amounts, and the plain white envelopes first used to mail tickets to violators. The city acknowledged the vendor's software problems but that was little relief for numerous motorists who received the citations. During the first month of the new rollout, at least 14,481 motorists got tickets, and 6,700 avoided tickets by paying for more time. The city did not provide its collections rate under the new system. Mike McConnell, *Royal Oak working with parking meter contractor to fix glitches*, Royal Oak Daily Tribune, (January 26, 2022, 5:14 P.M.).

[45] In Worcester, England, 1,500 motorists had their bank accounts overdrawn by hundreds of pounds after their contactless cards were repeatedly debited by a council's parking payment machines. Some were unable to pay their bills after the software glitch charged their card multiple times. Anna Tims, *Contactless cards were repeatedly debited by council's payment machines, in one case up to £600*, The Guardian, (October 5, 2022, 7:29 AM)

[46] *Id.* p. 4

[47] *See* Electronic Frontier Foundation. *Street Level Surveillance: Automatic License Plate Readers*, accessed on November 18, 2022.

[48] Angel Diaz & Rachel Levinson-Waldman, *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use*, Brennan Center for Justice, (September 10, 2020).

[49] Mr. Ford provided the *Progressive Parking Initiative Whitepaper* to the team which analyzed parking enforcement equity within Oakland. The paper was produced by a student who assisted DOT in convening a working group to assess and develop plans for parking fines and fees reforms. The paper found significant inequities in parking enforcement and citation between higher and lower income neighborhoods, of which the latter had high Black, Latinx and Asian populations. The paper provided several recommendations to reduce the impact of parking enforcement on lower income communities, of which only two appear to have been adopted by DOT, i.e., implementing an income payment plan for citations and enfolding scofflaw and abandoned auto into the transportation department.

[50] *See* "Draft Anticipated Impact Report: Mobile Parking Payment Systems for Parking Management and Enforcement," p.10

the ALPR that it "will conduct annual audits of ALPR data to ensure a reasonable standard of data accuracy and to verify that operators and administrators are following use policies."

Annual audits will be insufficient to mitigate the disproportionate harm on low-income or resource-poor residents who have neither the time nor the skill to correct misinformation with third party payment processors or successfully appeal citations. ALPRs should be designed and operated to check for routine errors and kept up to date, especially if third party payment providers are feeding information into the ALPRs that can lead to erroneous citation issuances.[51]

In the white paper mentioned above, one survey respondent, who is an East Oakland resident working full time, a student and living with a disability obtained several parking tickets.[52] They described their experience to both enroll in a payment plan for past due parking violations and to contest clearly erroneous citations. They were unable to afford the plan or successfully appeal invalid citations. If DOT can do more to ensure real-time accuracy of the system, monitor app updates, and clearly specify how drivers can correct misinformation, it will reduce the number of individuals adversely impacted by misidentifications. Additionally, there are second-order effects from the use of ALPR-mounted vehicles being deployed in high-poverty areas, namely residents' ability to pay outstanding fines.

Recommendation 5: Improve Equity in City-Managed Payment Plans for Parking Citations, Fines, Fees & Penalties

A December 2019 *Mercury News* article, entitled "The Bay Area's 10 poorest neighborhoods,"[53] identified at least six zip codes in Oakland, California, as experiencing the highest poverty in the region. Those zip codes – 94621, 94601, 94607, 94612, 94606, and 94603 – coincidentally are in areas that DOT has significant parking meters and will eventually be targeted for ALPR-deployment, as indicated by the following OAKGIS map here. Although Mr. Ford has indicated that ALPR-mounted vehicle deployment is at 60 percent capacity (or 4 out of 7 vehicles), and the PCTs are primarily focused on commercial districts and gateless garages, the high number of parking meters in poor areas still makes it very likely poorer residents will be adversely impacted. Even if poorer residents are not cited in their communities, they are still affected in other areas of Oakland they frequent. DOT presumes that poorer residents do not frequent commercial districts for work, shopping, and socializing. In fact, when individuals' communities have affordable housing, but lack suitable employment, they are *more* likely to work in and commute to richer, commercial districts, primarily for retail and restaurant jobs.[54]

---

[51] *See* Second Report of the Axon AI & Policing Technology Ethics Board: Automated License Plate Readers, October 2019

[52] *Supra note* 50, *Progressive Parking Initiative Whitepaper*, p. 12

[53] Kaitlyn Bartley, *The Bay Area's 10 Poorest Neighborhoods*, Mercury News, (December 8, 2019, 3:28 P.M.)

[54] Blumenberg and Wander tested the relationship between the availability of affordable housing relative to jobs and commute distance in two diverse metropolitan districts in Southern California; Los Angeles-Orange and Riverside-San Bernardino. There was a worse "fit" between the number of low-wage jobs and affordable housing rentals in longer commute districts in LA-Orange than Riverside-San Bernardino, a lower cost, inland, newer and more suburban area. In higher cost cities, lower-income residents are forced to move further from work to find affordable housing and commute longer to job-rich areas. The study suggested there are now more lower-income residents in the suburbs than urban, metropolitan cities because there is more affordable housing. However, jobs have not relocated to suburban areas around LA-Orange, forcing residents to travel further. In Cleveland, Ohio, the opposite is true.Due to suburban sprawl, urban residents must commute to suburban areas for jobs and amenities because

The prevalence – or lack thereof – of jobs, retail, and grocery stores in poorer communities is highly determinative of someone's ability to stay closer to home, and avoid parking citations at meters or contactless payment systems.

It is impossible to identify the exact racial demographics of all motorists, or even where they accumulate most of their parking citations, but it is clear that a person's zip code is highly determinative of their likelihood to be cited and booted and afford their fines. As of 2019, the zip code data for most towed scofflaw vehicles were in Fruitvale and West Oakland.[55] Census data for Fruitvale, or the 94601-zip code, showed there was a median income of $53,433, an employment rate of 58.3%, a poverty rate of 23% and at least 11.3% of people without health insurance. And one of the zip codes for West Oakland, 94607, had a median household income of $60,181, an employment rate of 63.9%, a poverty rate of 22.2% and at least 6.6% of people without health insurance. Residents living in both zip codes earned less than the state's median income of $84,907, and had higher poverty rates than the state average of 12.3%. As the current parking citation fees described below show, and the white paper confirmed, most residents cannot afford to pay one, let alone numerous, citations.

Oakland's most common parking violations include an expired meter ($58 fee violation);[56] failure to display a parking receipt ($58 fee violation);[57] parking in a red zone ($83 fee violation);[58] parking in a bus zone ($265 fee violation);[59] and failure to cramp wheels on grade ($45 fee violation),[60] among others.[61] And, between 2014 and 2019, many motorists were cited for failing to remove their cars on street sweeping days, resulting in 940,479 tickets being issued.[62] In 2018, the City issued 174,392 tickets for street sweeping and collected more than $11 million dollars in revenue from that category of citations.[63] With these high rates of citations, motorists can apply for two parking ticket payment plans: 1) income driven payment plans; and 2) a traditional payment plan to help them avoid being booted, towed and subject to driver registration problems. To qualify for the income driven payment plan, residents must either receive public benefits or be extraordinarily low income, and have no more than $250 in monthly disposable income.[64] Family income is capped at very low levels and disqualifies many residents in the aforementioned zip codes because they make above the family income caps for each family size. For example, a two-person family's gross monthly household income (before tax deductions) cannot exceed $4,567, or $54,804 annually, which sits below the median income for

---

workforce development, retail and other amenities have been concentrated in the suburbs. In general, whenever the cost of living pushes up housing prices in certain areas and continues to concentrate jobs and amenities in those locations, poorer residents must move to places with affordable housing and travel longer for work and other services. *See* Blumenberg, E. & Wander, M. *Housing affordability and Commute Distance.* Institute of Transportation Studies, University of California, Los Angeles, (June 15, 2022); *See also* Jay Miller, *Job Sprawl Spillover*, Crain's Cleveland Business, (July 25, 2022)

[55] *Supra note* 50, *Progressive Parking Initiative Whitepaper*, p. 11

[56] Oakland Municipal Code (OMC) 10.36.050

[57] OMC 10.36.050B

[58] OMC 10.40.020A1

[59] OMC 10.40.090E

[60] OMC 10.16.090

[61] *See* City of Oakland, Department of Transportation for additional common parking violations and ticket fees.

[62] *Supra note* 50, *Progressive Parking Initiative Whitepaper*, p. 10

[63] *Supra note* 50, *Progressive Parking Initiative Whitepaper*, p. 11

[64] *See* "City of Oakland: Request for Ability to Pay Determination Form"

the 94607-zip code. Moreover, the income payment plan does not add on new tickets, is at the discretion of DOT, and requires strict income and identity verification requirements. If the income driven payment plan is defaulted, "all penalties and interest will be applied to each citation, [along with] a collection fee of $300 or 10%, whichever is greater, will be assessed on the unpaid balance and collections action" will be immediate.[65]

The traditional payment plan allows individuals with higher incomes and disposable income, as well as parking citations exceeding $250, to apply.[66] However, there is a payment plan set-up fee added to the ticket amount, a 50% down payment due at the start of the plan, and significant identity verification during the application process.[67] Valid identification includes submission of a recent pay stub, or a completed 1040 tax return plus the last three months of bank statements for self-employed workers, a copy of a valid driver's license or passport, and a copy of a social security card.[68] Persons receiving unemployment, disability, SSI, SSA or any other type of assistance must provide an income statement and monthly expenses or have a cosigner.[69] Both payment plans are onerous to apply for, require significant paperwork and verification, and have steep penalties for inability to pay once the plan is in place. These plans are insufficient to help residents mitigate outstanding fines and avoid heavy driving penalties, including registration problems and other driving infractions.

Ironically, DOT and the Department of Race and Equity and the Civic Design Lab (CDL) worked to create a progressive payment system for parking fines and fees. They used an equity centered analysis and a human centered design process. They engaged residents through surveys and in-person groups to reimagine how a parking enforcement system could look.[70] Sixty percent of the 435 survey respondents noted they had received at least one parking citation in the last 12 months and 56 people had participated in a payment plan.[71] 61 percent of people, or 34 respondents, participating in the payment plan did not complete it, 21 percent had their vehicle towed or booted, and 30 percent were not able to get their car back.[72] Although these were self-reports, it showed that the then-existing payment schedule was impossible for several people. The newer plans, including the income-based version, do not appear to be any better. The report's recommendation on payment plan accessibility provided that the City set payment plans according to HUD's financial qualification rubric and incorporate considerations for financial costs of living in the Bay Area. This memo supports that recommendation and calls for the City to specifically revise the maximum monthly disposable income limit for the income-based payment plan upward to at least $650, to account for households earning *less* than the state's median income but *more* than the currently prescribed income limits.

Recommendation 6: Eliminate Consequences for Unpaid Parking Violations and Impact on Other Driving Privileges

[65] *See* "City of Oakland: Request Parking Ticket Payment Plan"
[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] *Supra note* 50, p. 8
[71] *Supra note* 50, p. 9
[72] *Id.*

When motorists fail to pay their traffic citations and/or do not complete payment plans, their driver's registration can be blocked and they can accrue additional penalties and interest. Under California Vehicle Code (CVC) §§ 4760 and 4761 a motorist cannot renew their registration if they have unpaid parking or toll violations on record.[73] *All* violations must be cleared by the issuing agency, i.e., DOT, or paid with the renewal fees before the renewal can be completed. Additionally, if a motorist claims a citation was issued erroneously, they must resolve their claim with the parking agency. The California DMV does not have authority to remove the citation without a release from the issuing parking agency or payment of the violation fine. Therefore, a motorist who either willfully or mistakenly acquires a parking citation, because of PCT error or a malfunctioning mobile parking application, has several procedural steps to resolve the citation, beginning with DOT or directly with the vendor. If the motorist cannot successfully resolve their parking citations, they will eventually have an invalid registration and be subject to further infractions, penalties, and costs. *See* CVC §4000a1.[74] There are several ways that DOT can reduce the likelihood of motorists accumulating related infractions and penalties stemming from unpaid parking citations by modeling efforts in other states.

Many states have reduced penalties for failing to pay parking tickets. In New York and New Jersey, failure to pay parking citations used to result in suspended licenses and criminal penalties for drivers who continued driving. In 2021, New York passed the Driver's License Suspension Reform Act that ended the practice of suspending licenses for unpaid traffic fines and fees, including parking citations.[75] The state's DMV automatically lifted all suspensions of driver's licenses, privileges to operate, and registrations for unpaid traffic fines and fees. Moving forward, New Yorkers who cannot pay their traffic fines, fees and mandatory surcharges will be able to pay $25/month or 2 percent of their net monthly income, whichever is greater. In 2020, Illinois Governor J.B. Pritzker signed legislation that ended the practice of suspending licenses over unpaid parking tickets.[76] The law, License to Work, allowed more Illinois motorists to drive legally and prevented them from losing their licenses for reasons that had nothing to do with driving, including standing and vehicle compliance violations. A New Jersey bill, A136, would model Illinois's initiative by eliminating license suspension as a punishment for nonpayment of traffic tickets; however, blocked registration would still be a legal penalty.[77] A Marketplace article found that in more than 40 states people can lose their license for non-driving infractions, including unpaid court costs, parking tickets and forgetting court dates.[78]

In Ohio, more than one million people, many of whom were poor and working-class, had their driver's licenses suspended for various traffic and parking offenses.[79] The expensive court

---

[73] *See* California Department of Motor Vehicles (DMV) Vehicle Industry Registration Procedures Manual, accessed on November 25, 2022

[74] The specific penalty schedule can be found at the California DMV website on "Penalties."

[75] Morgan McKay, *NY Driver's Licenses Will No Longer Be Suspended for Unpaid Fines*, Spectrum News 1, (June 29, 2021, 8:17 P.M.)

[76] Melissa Sanchez, ProPublica, and Elliot Ramos, WBEZ Chicago, *Tens of Thousands of People Lost Driver's Licenses Over Unpaid Parking Tickets. Now, They're Getting Them Back*, ProPublica, (Jan 17, 2020, 3:26 P.M.)

[77] Sophie Nieto-Munoz, *Bill Would Stop Driver's License Suspensions Over Unpaid Parking Tickets*, New Jersey Monitor, (Feb 3, 2022, 6:51 A.M.)

[78] Nadege Green, *Many States Still Suspend Driver's Licenses for Unpaid Fines That Are Not Related to Driving*, MarketPlace, (Sept 25, 2019)

[79] M.L. Schultze, *Ohio Offers A Second Chance to Drivers Struggling to Reinstate Their Licenses*, WKSU, (December 24, 2019, 5:35 A.M.)

fines and fees, as well as driver license reinstatement fees, prevented them from re-obtaining their licenses. Through House Bill 285, Ohio implemented and made permanent a driver's license amnesty program that required the Bureau of Motor Vehicles (BMV) to automatically notify, by either regular mail or email, drivers who qualified for the program. The program granted fee reductions or total waivers of license reinstatement fees owed to the BMV for driving while under suspension and if the suspension was due to an eligible offense.[80] Under current Ohio law, if a person's license was suspended for an eligible offense, it had been 18 months since the suspension and they had completed all court-ordered sanctions, they could be eligible for a complete or partial waiver of reinstatement fees, depending upon their level of indigency and receipt of public benefits. California had a similar driver's amnesty program which was authorized by Governor Jerry Brown in 2015 but it expired in 2017.[81]

DOT should strongly consider the financial, civil, and criminal implications for increased ALPR deployment and inflexibility in its payment plans. It can encourage the Oakland City Council to create a local driver's amnesty program that allows a portion of outstanding parking fines to be completely forgiven in exchange for community service at a local food bank or another volunteer effort. Where community service would be difficult for working adults and parents, the city could allow individuals making up to 200% of their zip code's median income to have 25 to 50 percent of their outstanding fines forgiven in a one-time effort. And, it can create the greatest payment flexibility for low-income motorists in its current income driven payment plan, by raising the income caps that qualify. However, the payment plan, by itself, makes it nearly impossible to comply with the payment terms without significant consequences. Mr. Ford revealed the city has $30 million in uncollected citations, exclusive of payment plans. Between 2011 and 2016, DOT issued 1,566,409 tickets, worth $108 million in citation revenue and $61 million in penalties for unpaid tickets.[82] Although statistical data is not available to estimate how many of those motorists eventually had their vehicle registration blocked or were cited for driving without a valid registration due to an unpaid citation, it is presumed to be significant.

In January 2021, California lifted suspensions for more than a half million motorists, most who had their license suspended for failure to appear in court.[83] The lawsuit that helped motorists have their licenses reinstated claimed that a disproportionate of those suspensions were born by low-income residents and communities of color. In any given year, California issues more than three million infraction citations, averaging between $600 and $700 each, some of which most likely stemmed from unpaid parking citations. Finally, California has among the highest traffic ticket penalties in the country due to state and county add-on fees. The City and DOT can lessen the burden on low-income motorists by instituting a local driver's amnesty program; conducting more frequent audits of vendor's mobile parking apps to ensure errors and

[80] Eligible offenses included operating vehicle without proof of insurance (ORC 4509.101), failure to pay security deposit, regarding a motor vehicle accident (ORC 4509.17), repeat traffic offender (ORC 4510.037), and failure to appear or failure to pay a fine related to specific vehicle-related offenses (ORC 4510.22), among others.
[81] California Courts, The Judicial Branch of California, "Traffic Tickets, Infractions Amnesty Program," accessed on November 20, 2022, website: https://www.courts.ca.gov/trafficamnesty.htm?rdeLocaleAttr=en
[82] *Supra note* 50, p. 10
[83] *See* Robert Lewis, *State Lifts Suspension of Half a Million Driver's Licenses*, Cal Matters (Jan 29, 2021). *See also* Rebecca Miller, *California Stopped Suspending Licenses for Failure to Pay Traffic Fines*, Western Center on Law and Poverty, (May 13, 2019).

updates do not erroneously result in driver's receiving citations; easing eligibility requirements for payment programs; and decreasing penalties for an inability to pay or missed payments. DOT may even conduct an audit to determine the cause of the uncollected citation fees. An audit may find that much of it relates to individuals' low socioeconomic status. Other mitigation measures that DOT can consider to offset parking policing is limiting data sharing with local, state and federal law enforcement authorities and other municipal agencies.

Recommendation 7: Create Written Protocols for ALPR Data Sharing with Other Law Enforcement

DOT stated in the 2019 AIR for vehicle-mounted ALPRs that it "will not share ALPR data with the Police Dept., DMV, Law Enforcement Agencies, other cities' jurisdictions, *except* **[emphasis added]** when "hit" data is used as evidence in support of parking violations."[84] Mr. Ford provided some assurance that ALPR information related to scofflaw and abandoned vehicles would not be shared with law enforcement because those functions were being integrated into DOT, per the recommendations of the 2019 white paper published three years ago. However, this integration does not change the fact that parking enforcement, regardless of which agency does it, is still policing and results in significant financial harm to certain communities. The integration also does not negate the possibility that DOT's ALPR system will not be *connected* with other law enforcement management systems and still generate high error rates.

A second report of the Axon AI & Policing Technology Ethics Board recommends ALPRs that register "hits" should not notify law enforcement to a motorist's vehicle if it is to enforce civil infractions, offenses enforceable by citation, or outstanding warrants arising out of a failure to pay fines and fees.[85] The sharing of ALPR data by DOT with other government agencies should be subject to well defined data sharing protocols, and should be consistent with California's ALPR legislation. Moreover, DOT needs to be transparent with potential parkers so that they are aware of the ALPR data being collected, what it can be used for, and with whom it can be shared. This means publishing a notice on its own website and/or getting the mobile parking providers to publish a notice on their portals on behalf of the DOT. (*See* Bureau of Automotive Repair (BAR) ALPR Use Policy as a sample policy in Appendix D.) With public notice, customers should be aware that if their vehicle becomes subject to scofflaw this data could be shared with state authorities.

Mr. Ford mentioned in an October 21 conversation with students that he wanted to integrate stolen vehicle data into the California Law Enforcement Communications System (CLECS). CLECS would be integrated into Conduent and ALPRs and, presumably, accessed by PCTs during enforcement activities. To complete this integration, Mr. Ford would have to complete training and certification with the Department of Justice to gain access to the CLECS database. While it may help owners recover their stolen vehicles more quickly, it presents the

[84] *Supra note* 17

[85] *See* "Second Report of the Axon AI & Policing Technology Ethics Board: Automated License Plate Readers," Axon AI, p. 8, accessed at: https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5dadec937f5c1a2b9d698ba9/1571679380452/Axon_Ethics_Report_2_v2.pdf

opportunity for increased misidentification and error on stolen vehicles via Conduent or ALPRs, and additional fees being generated for motorists to recover their stolen vehicles from impound yards. The 2019 white paper addressed motorists' frustration with having to pay a fee to recover their stolen vehicles and recommended any recovery fee be waived. It is unknown if DOT has adopted a fee waiver for owners of stolen vehicles.

When considering fee waivers, improved payment plans, or other recommendations on racial equity provided in this report, DOT should provide them to the new program analyst for racial equity. The analyst can help the city reduce disproportionate harm by having access to this memo and other research done on behalf of DOT, including the recommendations from the East Bay Community Law Center. In total, these recommendations on racial equity should be strongly considered to reduce the disproportionate financial harm of fines and fees on vulnerable communities in Oakland.

Recommendation 8: DOT should make available to the parking public, in a transparent way, its own privacy policy in regard to ALPR and other enforcement-related personal information, following the CCPA requirements as best practice.

It is important for the DOT to be transparent with motorists that are using its parking facilities, so that they are aware of the ALPR data being collected, what it can be used for, and with whom it can be shared, within the City of Oakland or other government authorities, and with other third parties, including service providers. This means publishing a notice on its own website and/or requiring the mobile parking providers to publish a notice on their portals on behalf of the DOT. The public notice should take into consideration the privacy notice/policy requirements of the CCPA as a best practice to follow. For example, parking customers should be aware that if their vehicle becomes subject to scofflaw penalties, this data could be shared with state authorities. The DOT should include in its privacy notice information about how data collected by third party providers on its behalf is aggregated and used, to the extent that this information is not covered in the Providers' own privacy policies (as discussed above in relation to Recommendation #3. An example of an ALPR Privacy and Use Policy, published by the Bureau of Automotive Repair in June 2021, may be found at: https://www.bar.ca.gov/ALPR .

V. Conclusion

The implementation of a complex multi-provider payment parking system is an ambitious and meaningful step forward to provide parkers in the City with a range of options and allow the City to more effectively manage a limited and important resource. However, with opportunity comes responsibility. As outlined above, the City and DOT have a responsibility to address critical issues and concerns regarding data privacy and equitable enforcement. It is with this in mind, that we share our above analysis and recommendations for both the City and PAC to review, discuss with the appropriate counsel, and consider incorporating into the System's implementation plan.

Key Acronyms

- Automated License Plate Reader (ALPR)
- Anticipated Impact Report (AIR)

- California Consumer Privacy Act (CCPA)
- California Privacy Rights Act (CPRA)
- California Law Enforcement Communications System (CLECS)
- Department of Transportation (DOT)
- Mobile Payment Providers ("Providers")
- Oakland Police Department (OPD)
- Parking Control Technician (PCT)
- Performance Service Agreement (PSA)
- Privacy Advisory Commission (PAC)
- Residential Parking Permits (RPPs)
- Surveillance Impact Report (SIR)
- Surveillance Use Policy ("Use Policy")

Appendix Contents

Appendix A - Draft Package from July 2022 of documents re: Mobile Payment Parking Systems, including:

- Draft Proposed use policy, dated 7/7/2022
- Draft Anticipated Impact Report, dated 7/7/2022
- Draft Proposed Use Policy, dated 5/6/2021
- Appendix A for Mobile Parking Payment System, dated March 2022 (this looks like the RFP that went out)
- Appendix B - Providers Privacy Policies (Passport, Pay by Phone, ParkMobile, IPS Group, Honk Mobile)
- Appendix C - Providers' User Terms and Conditions (IPS Group, Honk Mobile, Pay by Phone, Passport, ParkMobile)
- Appendix D - Existing Professional Services Agreement Language

Appendix B - CCPA Presentation from Ann LaFrance
Appendix C - Data Map
Appendix D - Bureau of Automotive Repair (BAR) Automated License Plate Reader Privacy & Use Policy
Appendix E - Providers' Privacy Policy Summaries
Appendix F - Executed ParkMobile Professional Services Agreement
Appendix G - Draft Mobile Parking App Professional Services Agreement language
Appendix H - Oakland Professional Services Agreement Sample
Appendix I - 2019 Dockless Mobility Data Sharing Recommendation to Adopt a Resolution (draft and final)
Appendix J - 2019 Dockless Mobility Data Sharing Resolution (draft and final)
Appendix K - Dockless Mobility Data Sharing Impact Report
Appendix L - Dockless Mobility Data Sharing Use Policy
Appendix M - Oakland Parking Enforcement Equity Analysis
Appendix N - Automated License Plate Reader Final Use Policy
Appendix O - Automated License Plate Reader Final Anticipated Impact Report
Appendix P - Bio of Brandon Green

Appendix Q - Progressive Parking Initiative Information and White Paper
Appendix R - Oakland City Council Surveillance Ordinance
Appendix S - Oakland Privacy Advisory Commission Bylaws
Appendix T - Oakland Privacy Advisory Commission Establishing Ordinance
Appendix U - Oakland Citywide Privacy Principles